DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNA

VICTOR ALFONSO GALVIS QUIROGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA SISTEMAS
BOGOTÁ
2020

DIPLOMADO DE PROFUNDIZACION CISCO
SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

VICTOR ALFONSO GALVIS QUIROGA

Diplomado de opción de grado presentado para optar el título de
INGENIERO DE SISTEMAS

DIRECTOR:
JOSE IGNACIO CARDONA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA SISTEMAS
BOGOTÁ
2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____
Firma del presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

BOGOTÁ, 23 de noviembre de 2020

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

INTRODUCCIÓN

Este documento presenta el desarrollo de los escenarios 1 y 2 de la prueba de habilidades prácticas CCNA, del diplomado de profundización CISCO en la herramienta de simulación Packet Tracer, esta herramienta nos permite diseñar y construir diferentes topologías de red, configurar dispositivos, insertar paquetes y evaluar su comportamiento. En estas prácticas se aborda todo lo relacionado con el diseño de las topologías propuestas y la configuración de los dispositivos.

A lo largo del desarrollo de los laboratorios, se trabajó sobre los diferentes modos en los Switch, al igual que la configuración de VLAN, interfaces, direccionamiento IP, usuarios, troncales, cifrado de contraseñas, EtherChannel, DHCP, NAT, NTP, ACL, etc. Al igual que la configuración y administración de Switch, Router, PC y demás dispositivos informáticos, garantizando su conmutación, enrutamiento y comunicación en las redes configuradas.

En el primer escenario nos enfocamos en la configuración de dispositivos, entre los cuales encontramos, Router, Switch, PC bajo el protocolo IPv4 e IPv6, se configuran los router y switch para ser administrados de forma segura, a la vez que se configura las VLAN correspondientes, se activan servicios de DHCP y se configura EtherChannel y port-security.

A diferencia del escenario anterior y adicional en el escenario 2, aplicamos configuraciones relacionadas con el protocolo OSPF, DHCP, NTP, establecemos listas de control ACL y se configuración la traducción de direcciones de red NAT.

En las evidencias podemos observar las configuraciones aplicadas, comandos utilizados y resultados obtenidos.

DESARROLLO

ESCENARIO 1

Figura 1. Escenario 1

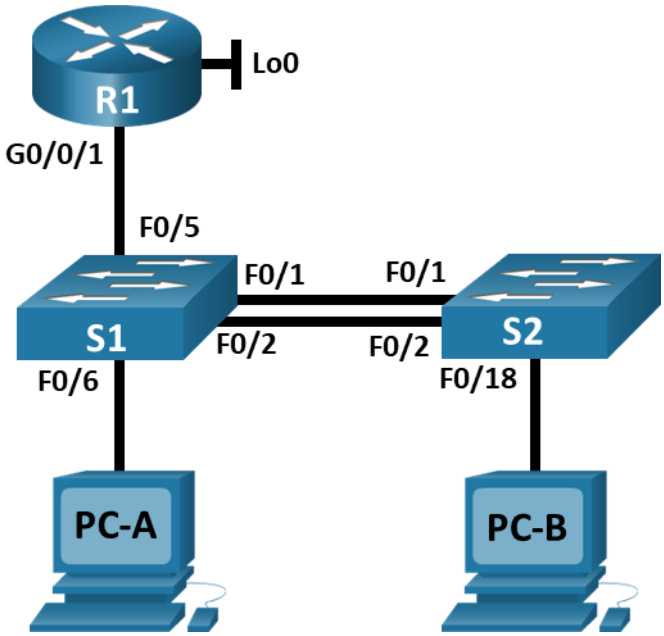
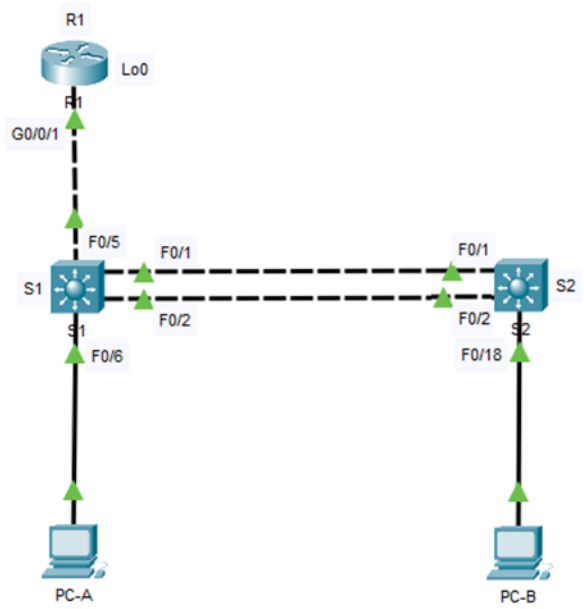


Figura 2. Simulación de escenario 1



1.1 Borre las configuraciones de inicio y las VLAN del router y del Switch y vuelva a cargar los dispositivos.

En este primer paso accedemos al router y a cada uno de los Switch para borrar las configuraciones que puedan haberse realizado, a continuación, anexo código.

Router

Router>en
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

Router#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
… RESULTADO OMITIDO
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: no
Press RETURN to get started!

Switch 1:

Switch>en
Switch#sh flash
System flash directory:
File Length Name/status
3 8662192 c3560-advipservicesk9-mz.122-37.SE1.bin
2 28282 sigdef-category.xml
1 227537 sigdef-default.xml
[8918011 bytes used, 55098373 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write)

Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

Switch#reload
Proceed with reload? [confirm]
… RESULTADO OMITIDO
% Please answer 'yes' or 'no'.
Would you like to enter the initial configuration dialog? [yes/no]: no
Press RETURN to get started!
Switch>

Switch 2:

Switch>en
Switch#sh flash
System flash directory:
File Length Name/status
3 8662192 c3560-advipservicesk9-mz.122-37.SE1.bin
2 28282 sigdef-category.xml
1 227537 sigdef-default.xml
[8918011 bytes used, 55098373 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write)

Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]

Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

Switch#reload
Proceed with reload? [confirm]
… RESULTADO OMITIDO
--- System Configuration Dialog ---
% Please answer 'yes' or 'no'.
Would you like to enter the initial configuration dialog? [yes/no]: no
Press RETURN to get started!
Switch>

1.2 Después de recargar el switch, configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch.

A continuación, Podemos ver con el comando “show sdm prefer” que la plantilla predeterminada es compatible con 8 interfaces enrutadas y 1024 VLAN, también observamos que no hay características IPv6 habilitadas:

Switch>en
Switch#show sdm prefer
The current template is "desktop default" template.
The selected template optimizes the resources in
the switch to support this level of features for
8 routed interfaces and 1024 VLANs.

number of unicast mac addresses: 6K
number of IPv4 IGMP groups + multicast routes: 1K
number of IPv4 unicast routes: 8K
number of directly-connected IPv4 hosts: 6K
number of indirect IPv4 routes: 2K
number of IPv4 policy based routing aces: 0
number of IPv4/MAC qos aces: 0.5K
number of IPv4/MAC security aces: 1K
Switch#

Con el comando “sdm prefer dual-ipv4-and-ipv6” activaremos la plantilla con opciones predeterminadas:

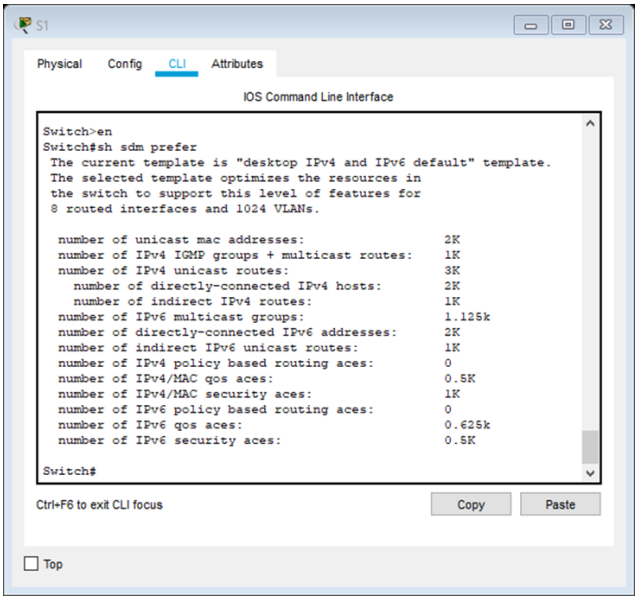
Switch 1:

Switch>
Switch>en
Switch#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#sdm prefer dual-ipv4-and-ipv6 default
Changes to the running SDM preferences have been stored, but cannot take effect until the next reload.
Use 'show sdm prefer' to see what SDM preference is currently active.
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#reload
System configuration has been modified. Save? [yes/no]:yes
Building configuration...
[OK]
Proceed with reload? [confirm]
… RESULTADO OMITIDO

Press RETURN to get started!

Figura 3. Verificación Plantilla SDM Switch1

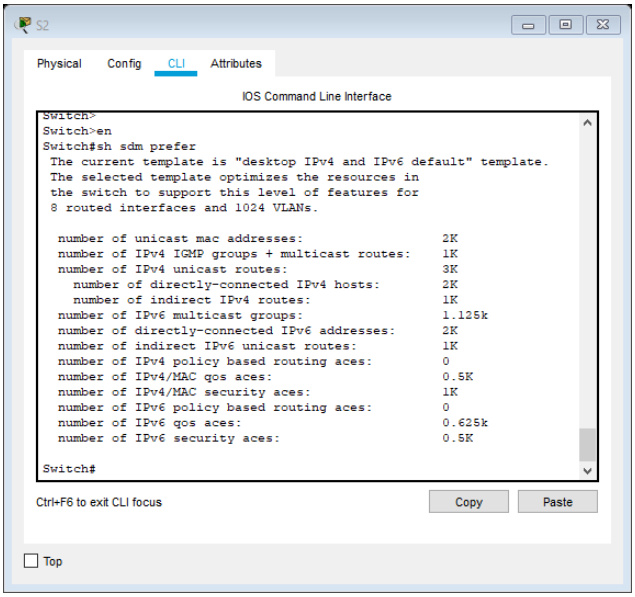


Switch2

Switch>
Switch>en
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#sdm prefer dual-ipv4-and-ipv6 default
Changes to the running SDM preferences have been stored, but cannot take effect until the next reload.
Use 'show sdm prefer' to see what SDM preference is currently active.
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#reload
System configuration has been modified. Save? [yes/no]:yes
Building configuration...
[OK]
Proceed with reload? [confirm]
… RESULTADO OMITIDO
Press RETURN to get started!
Switch>

Figura 4. Verificación Plantilla SDM Switch2



2.1 En este paso aplicamos las principales configuraciones en el Router, entre las cuales encontramos el cambio de nombre, asignación del nombre del dominio, configuración de las contraseñas para EXEC, consola y usuarios locales, además de la configuración de Routing IPV6, VTY, MOTD, Interfaces y RSA.

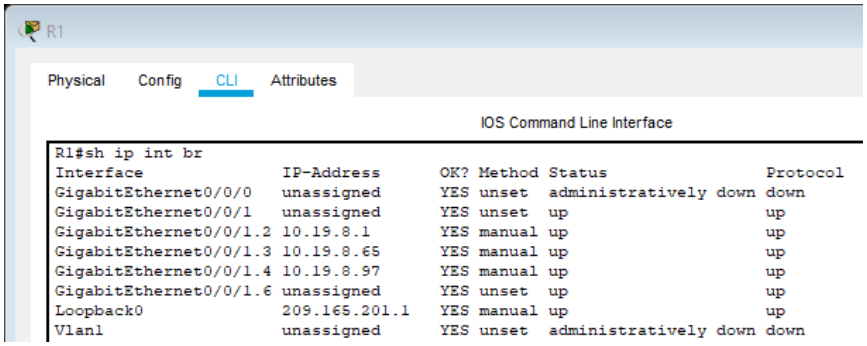
A continuación, se presentan en la siguiente tabla las configuraciones realizadas al R1:

Tabla 1 configuración inicial Router

Tarea	Especificación
Desactivar la búsqueda DNS	Router>en Router#config t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup Router#
Nombre del router	Router#config t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#hostname R1 R1(config)#
Nombre de dominio	Router#config t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#ip domain-name ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	Router#config t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#enable secret Ciscoenpass
Contraseña de acceso a la consola	Router#config t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#line con 0 R1(config-line)#password Ciscoconpass R1(config-line)#login R1(config-line)#exit R1(config)#

Establecer la longitud mínima para las contraseñas	Router#config t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#security passwords min-length 10
Crear un usuario administrativo en la base de datos local	R1#config t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#username admin password admin1pass R1(config)#
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local Configurar VTY solo aceptando SSH	R1#config t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#line vty 0 4 R1(config-line)# Login local R1(config-line)#transport input ssh R1(config-line)#exit R1(config)#
Cifrar las contraseñas de texto no cifrado	R1#config t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#service password-encryption R1(config)#
Configure un MOTD Banner	R1(config)#banner motd # Enter TEXT message. End with the character '#'. Zona Restringida por favor acceda con las credenciales suministradas# R1(config)#exit
Habilitar el routing IPv6	R1#config t Enter configuration commands, one per line. End with CNTL/Z. R1(config)#ipv6 unicast-routing R1(config)#

Configurar interfaz G0/0/1 y subinterfaces	R1>en R1 #config ter R1(config-if)# interface GigabitEthernet0/0/1 R1(config-if)# description ### Inside Network ### R1(config-if)# no ip address R1(config-if)# duplex auto R1(config-if)# speed auto R1(config-if)# ipv6 address FE80::1 link-local R1(config-if)# ipv6 enable R1(config-if)#end R1>en R1 #config ter R1(config)# interface GigabitEthernet0/0/1.2 R1(config- subif)# encapsulation dot1Q 2 R1(config- subif)# ip address 10.19.8.1 255.255.255.192 R1(config- subif)# ipv6 address 2001:DB8:ACAD:A::1/64 R1(config- subif)# ipv6 enable R1(config- subif)#end R1>en R1 #config ter R1(config)# interface GigabitEthernet0/0/1.3 R1(config- subif)# encapsulation dot1Q 3 R1(config- subif)# ip address 10.19.8.65 255.255.255.224 R1(config- subif)# ipv6 address 2001:DB8:ACAD:B::1/64 R1(config- subif)#end R1>en R1 #config ter R1(config)# interface GigabitEthernet0/0/1.4 R1(config-subif)# encapsulation dot1Q 4 R1(config-subif)# ip address 10.19.8.97 255.255.255.248 R1(config-subif)# ipv6 address 2001:DB8:ACAD:C::1/64 R1(config-subif)ipv6 enable R1(config-subif)#end R1>en R1 #config ter

	R1(config)#interface GigabitEthernet0/0/1.6 R1(config-subif)# encapsulation dot1Q 6 R1(config-subif)# no ip address R1(config-subif)#end Figura 5. Verificación de las interfaces en el Router 
Configure el Loopback0 interface	R1#config t R1(config)# interface Loopback0 R1(config-if)# description ### Interface Loopback ### R1(config-if)#ip address 209.165.201.1 255.255.255.224 R1(config-if)#ipv6 address FE80::1 link-local R1(config-if)# ipv6 address 2001:DB8:ACAD:209::1/64 R1(config-if)#end
Generar una clave de cifrado RSA	R1>en R1 #config t R1(config)# Crypto key rsa generate R1(config)# 1024 R1(config)#end

3.1 En este paso aplicamos las principales configuraciones a los Switch, entre las cuales encontramos el cambio de nombre, asignación del nombre del dominio, configuración de las contraseñas para EXEC, consola y usuarios locales, además de la configuración de VTY, MOTD, Interfaces y RSA.

A continuación, se presenta la configuración realizada a los Switch 1 y 2

Tabla 2 – configuraciones Iniciales S1 yS2

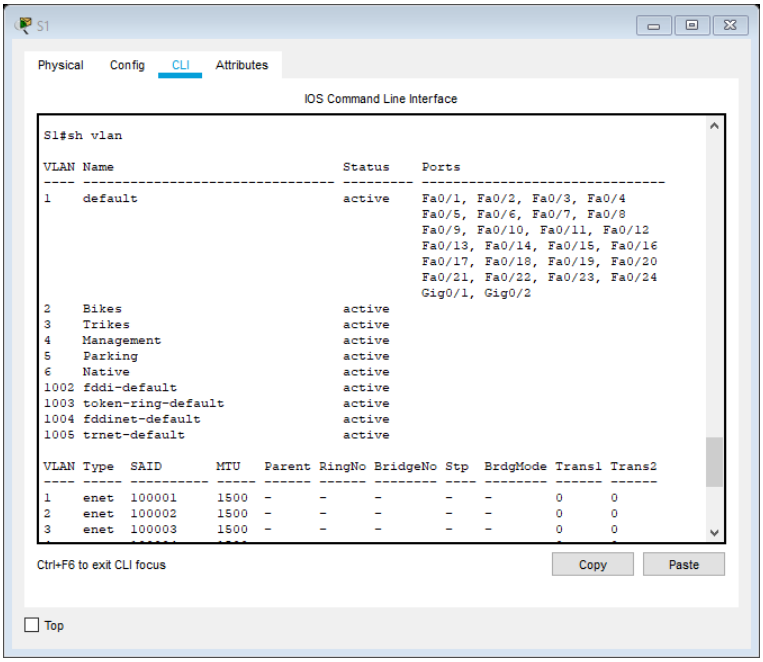
Tarea	Especificación
Switch 1: Desactivar la búsqueda DNS. Nombre del switch Nombre de dominio Contraseña cifrada para el modo EXEC privilegiado Contraseña de acceso a la consola Crear un usuario administrativo en la base de datos local Configurar el inicio de sesión en las líneas VTY para que use la base de datos local Configurar las líneas VTY para que acepten únicamente las conexiones SSH Cifrar las contraseñas de texto no cifrado Configurar un MOTD Banner Generar una clave de cifrado RSA	Switch>en Switch#config t Switch(config)#no ip domain-lookup Switch(config)#hostname S1 S1(config)#ip domain-name ccna-lab.com S1(config)#enable secret ciscoenpass S1(config)#line con 0 S1(config-line)#password ciscoconpass S1(config-line)#login S1(config-line)#exit S1(config)#username admin password admin1pass S1(config)#line vty 0 4 S1(config-line)#Login local S1(config-line)#transport input ssh S1(config-line)#exit S1(config)#service password-encryption S1(config)#banner motd # Enter TEXT message. End with the character '#'. Zona Restringida del Switch por favor acceda con las credenciales suministradas# S1(config)# Crypto key rsa generate S1(config)# 1024 S1(config)#end

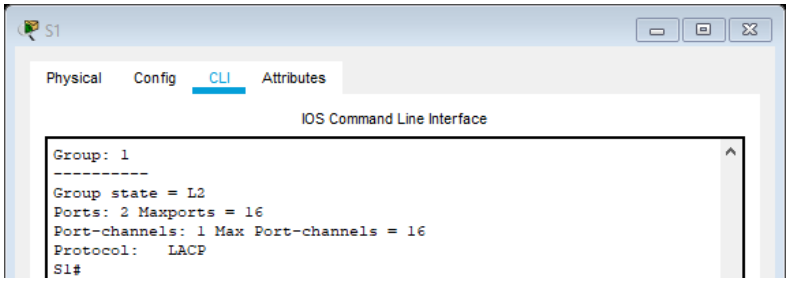
Switch 2: Desactivar la búsqueda DNS. Nombre del switch Nombre de dominio Contraseña cifrada para el modo EXEC privilegiado Contraseña de acceso a la consola Crear un usuario administrativo en la base de datos local Configurar el inicio de sesión en las líneas VTY para que use la base de datos local Configurar las líneas VTY para que acepten únicamente las conexiones SSH Cifrar las contraseñas de texto no cifrado Configurar un MOTD Banner Generar una clave de cifrado RSA	Switch>en Switch#config t Switch(config)#no ip domain-lookup Switch(config)#hostname S1 S2(config)#ip domain-name ccna-lab.com S2(config)#enable secret ciscoenpass S2(config)#line con 0 S2(config-line)#password ciscoconpass S2(config-line)#login S2(config-line)#exit S2(config)#username admin password admin1pass S2(config)#line vty 0 4 S2(config-line)#Login local S2(config-line)#transport input ssh S2(config-line)#exit S2(config)#service password-encryption S2(config)#banner motd # Enter TEXT message. End with the character '#'. Zona Restringida del Switch por favor acceda con las credenciales suministradas# S2(config)# Crypto key rsa generate S2(config)# 1024 S2(config)#end
Switch 1: Configurar la interfaz de administración (SVI) Configuración del gateway predeterminado	S1#config t S1(config)# interface Vlan4 S1(config-if)#ip address 10.19.8.98 255.255.255.248 S1(config-if)#ipv6 address FE80::98 link-local S1(config-if)#ipv6 address 2001:DB8:ACAD:C::98/64 S1(config-if)#ipv6 enable S1(config-if)#exit S1(config)# ip default-gateway 10.19.8.97 S1(config)#end
Switch 2: Configurar la interfaz de administración (SVI) Configuración del gateway predeterminado	S2#config t S2(config)#interface Vlan4 S2(config-if)#ip address 10.19.8.99 255.255.255.248 S2(config-if)#ipv6 address FE80::99 link-local S2(config-if)#ipv6 address 2001:DB8:ACAD:C::99/64 S2(config-if)#exit S2(config)# ip default-gateway 10.19.8.97 S2(config)#end S2(config)#

4.1 En este paso configuramos en el Switch 1, las diferentes VLAN, las troncales, el grupo de EtherChannel y los puertos de acceso.

A continuación, en la tabla se presentan las diferentes configuraciones realizadas al Switch 1:

Tabla 3 – Segunda configuración S1

Tarea	Especificación
Crear VLAN	S1#config t S1(config)#vlan 2 S1(config-vlan)#name Bikes S1(config)#vlan 3 S1(config-vlan)#name Trikes S1(config)#vlan 4 S1(config-vlan)#name Management S1(config)#vlan 5 S1(config-vlan)#name Parking S1(config)#vlan 6 S1(config-vlan)#name Native S1(config-vlan)#exit S1(config)# Figura 6. Verificación de las Vlan Creadas S1 

Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S1#config t S1(config)#interface FastEthernet0/1 S1(config-if)#switchport trunk native vlan 6 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport nonegotiate S1(config-if)#exit S1(config)#interface FastEthernet0/2 S1(config-if)#switchport trunk native vlan 6 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport nonegotiate S1(config-if)#exit S1(config)#interface FastEthernet0/5 S1(config-if)#switchport trunk native vlan 6 S1(config-if)#switchport trunk encapsulation dot1q S1(config-if)#switchport mode trunk S1(config-if)#switchport nonegotiate S1(config-if)#exit
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S1#config t S1(config)#interface fa0/1 S1(config-if)#channel-group 1 mode active S1(config-if)#exit S1(config)#interface fa0/2 S1(config-if)#channel-group 1 mode active S1(config-if)# exit Figura 7. Verificación del EtherChannel S1 
Configurar el puerto de acceso de host para VLAN 2	S1#config t S1(config)#interface f0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 2 S1(config-if)#no shut S1(config-if)#exit

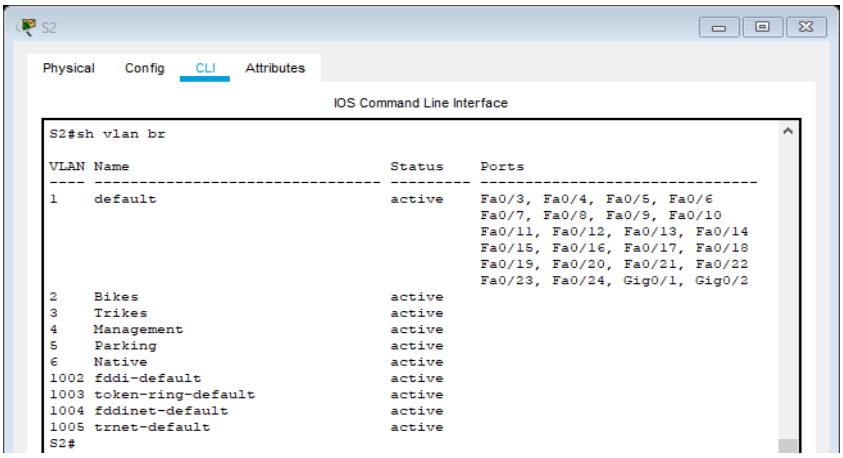
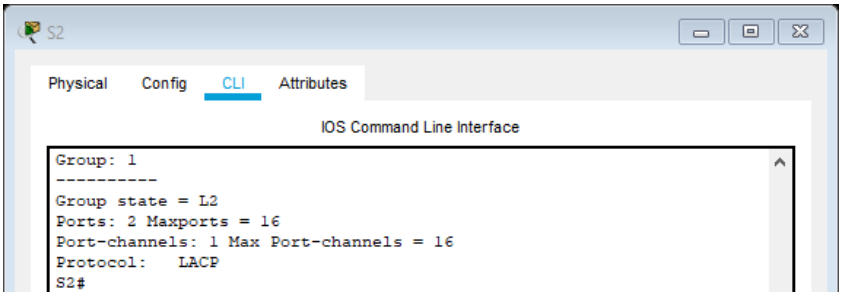
Configurar la seguridad del puerto en los puertos de acceso	S1#config t S1(config)#interface range fa0/1 - fa 0/24 S1(config-if-range)#switchport port-security S1(config-if-range)#switchport port-security maximum 3 S1(config-if-range)#switchport port-security violation protect S2(config-if-range)#exit
Proteja todas las interfaces no utilizadas	S1#config t S1(config)#interface range fa0/3-4, f0/7-24 S1(config-if-range)#description ##Puertos no utilizados## S1(config-if-range)#switchport access vlan 5 S1(config-if-range)#switchport mode access S1(config-if-range)#switchport nonegotiate S1(config-if-range)#switchport port-security S1(config-if-range)#switchport port-security maximum 3 S1(config-if-range)#switchport port-security violation protect S1(config-if-range)#Shutdown S1(config-if-range)#end

5.1 En este paso configuramos en el Switch 2, las diferentes VLAN, las troncales, el grupo de EtherChannel y los puertos de acceso.

A continuación, en la tabla se presentan las diferentes configuraciones realizadas al Switch 2:

Tabla 4 – Segunda configuración S2

Tarea	Especificación
Crear VLAN	S2(config)#vlan 2 S2(config-vlan)#name Bikes S2(config)#vlan 3 S2(config-vlan)#name Trikes S2(config)#vlan 4 S2(config-vlan)#name Management S2(config)#vlan 5 S2(config-vlan)#name Parking S2(config)#vlan 6 S2(config-vlan)#name Native S2(config-vlan)#exit

	Figura 8. Verificación de las VLAN creadas en el S2 
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	S2(config)#interface range f0/1-2 S2(config-if)#switchport trunk native vlan 6 S2(config-if)#switchport trunk encapsulation dot1q S2(config-if)#switchport mode trunk S2(config-if)#switchport nonegotiate S2(config-if)#end
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	S2(config)#interface range f0/1-2 S2(config-if-range)#channel-group 1 mode active S2(config-if-range)#end Figura 9. Verificación del EtherChannel en el S2 
Configurar el puerto de acceso del host para la VLAN 3	S2#config t S2(config)#interface f0/18 S2(config-if)#switchport mode access S2(config-if)#switchport access vlan 3 S2(config-if)#exit
Configure port-security en los access ports	S2#config t S2(config)#interface range fa0/1 - fa0/24 S2(config-if-range)#switchport port-security S2(config-if-range)#switchport port-security maximum 3 S2(config-if-range)#switchport port-security violation protect S2(config-if-range)#end

Asegure todas las interfaces no utilizadas.	S2(config)#interface range fa0/3-17, f0/19-24 S2(config-if-range)#description ##Puertos no utilizados## S2(config-if-range)#switchport access vlan 5 S2(config-if-range)#switchport mode access S2(config-if-range)#switchport nonegotiate S2(config-if-range)#switchport port-security S2(config-if-range)#switchport port-security maximum 3 S2(config-if-range)#switchport port-security violation protect S2(config-if-range)#Shutdown S2(config-if-range)#exit

6.1 a continuación se deben aplicar configuraciones adicionales al Router, estas configuraciones son relacionadas con Routing y DHCP:

Tabla 5 – configuraciones adicionales Router

Tarea	Especificación
Configure Default Routing	R1>en R1#config t R1(config)# ip route 0.0.0.0 0.0.0.0 Loopback0 R1(config)# ipv6 route ::/0 Loopback0 R1(config)#end
Configurar IPv4 DHCP para VLAN 2	R1>en R1#config ter R1(config)#ip dhcp pool VLAN2 R1(dhcp-config)#network 10.19.8.0 255.255.255.192 R1(dhcp-config)#default-router 10.19.8.1 R1(dhcp-config)#domain-name ccna-a.net R1(dhcp-config)#exit R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52 R1(config)#end

Tarea	Especificación
Configurar DHCP IPv4 para VLAN 3	R1>en R1#config ter R1(config)#ip dhcp pool VLAN3 R1(dhcp-config)# network 10.19.8.64 255.255.255.224 R1(dhcp-config)#default-router 10.19.8.65 R1(dhcp-config)#domain-name ccna-b.net R1(dhcp-config)#exit R1(config)# ip dhcp excluded-address 10.19.8.65 10.19.8.84 R1(config)#end

6.2 a continuación se presenta la configuración de los Host PC-A y PC-B, a nivel de direccionamiento IP:

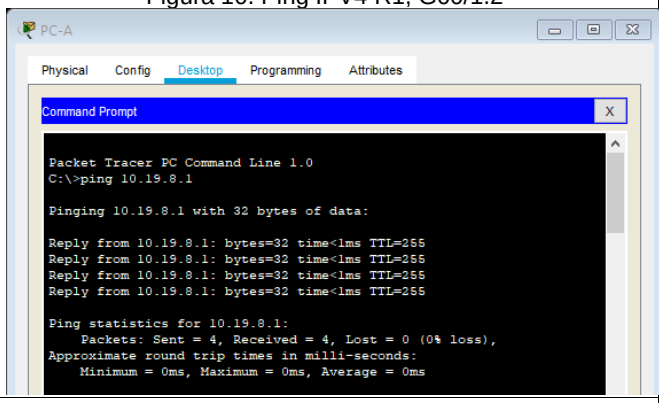
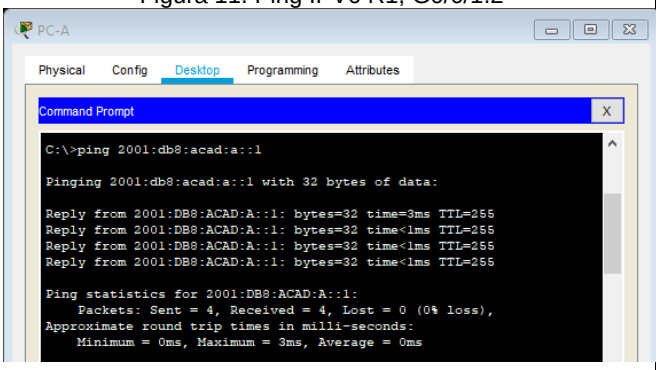
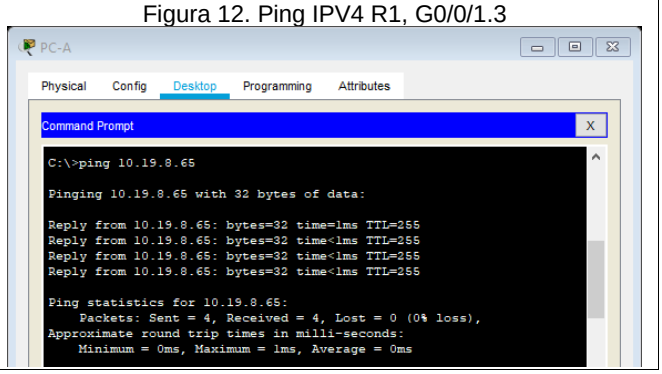
Tabla 6 – Configuración Host PC-A y PC-B

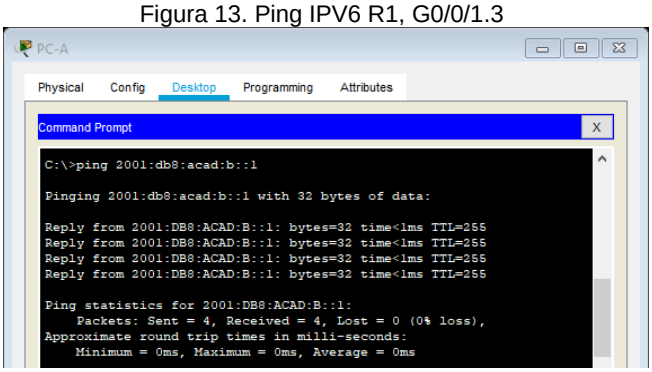
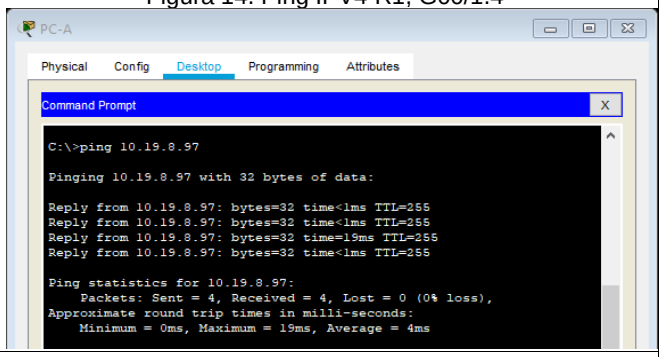
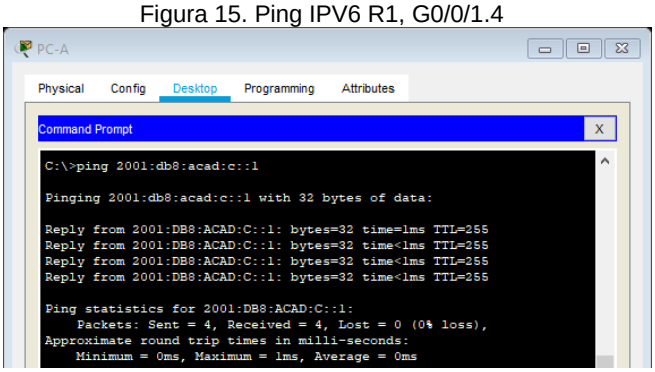
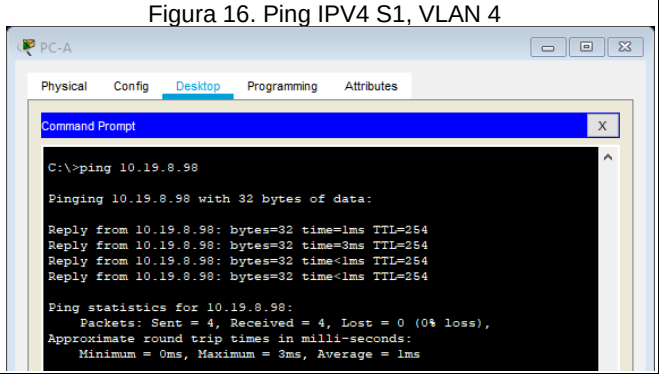
PC-A Network Configuration	
Descripción	PC-A
Dirección física	0010.11CB.B17E
Dirección IP	10.19.8.53
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

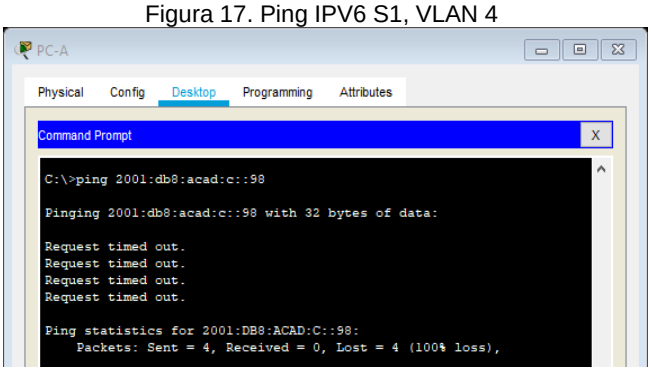
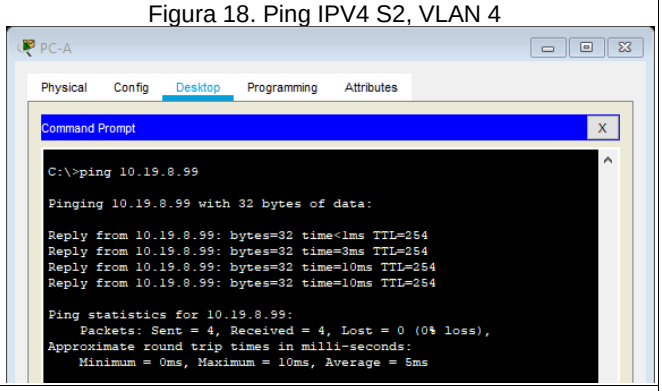
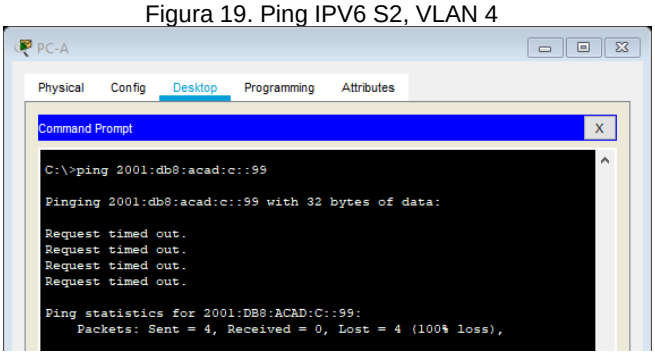
PC-B Network Configuration	
Descripción	PC-B
Dirección física	0009.7C8D.EA66
Dirección IP	10.19.8.86
Máscara de subred	255.255.255.224
Gateway predeterminado	10.19.8.65
Gateway predeterminado IPv6	2001:DB8:ACAD:B::1

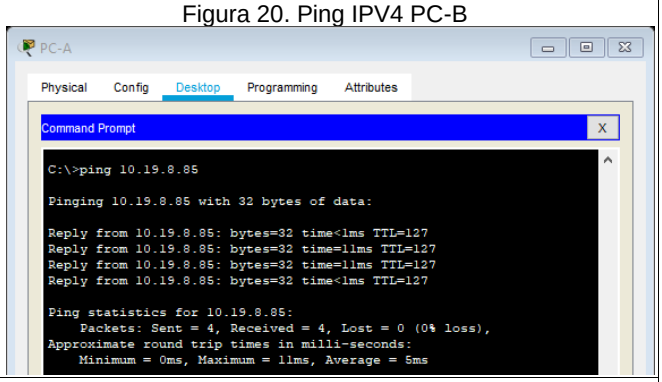
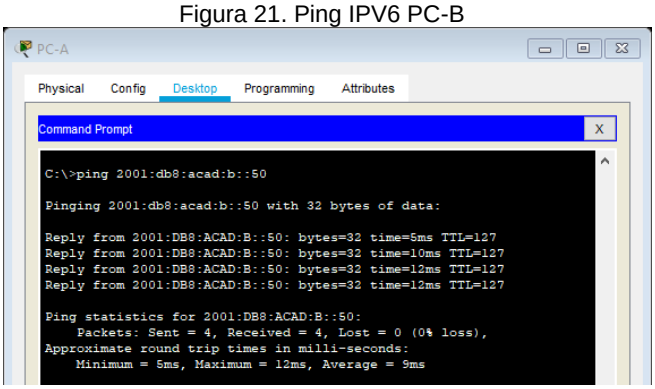
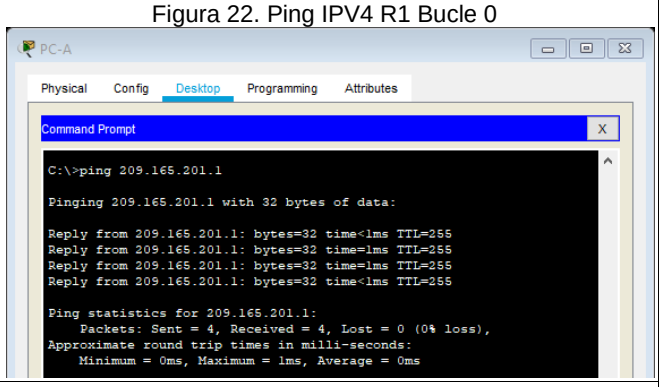
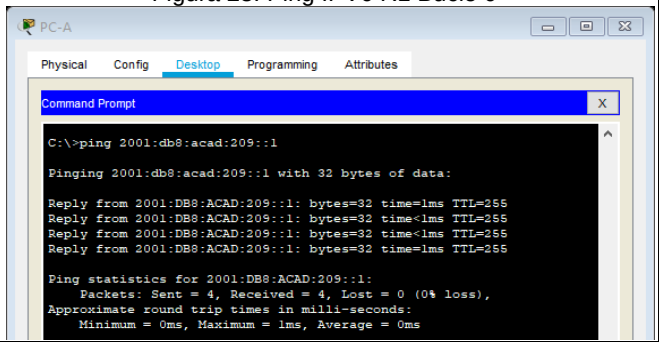
6.3 A continuación se ejecutan pruebas de conectividad, con el objetivo de realizar validaciones a nivel de comunicación y configuraciones:

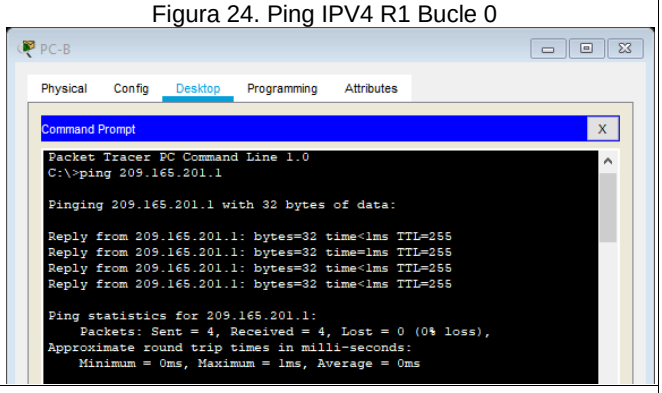
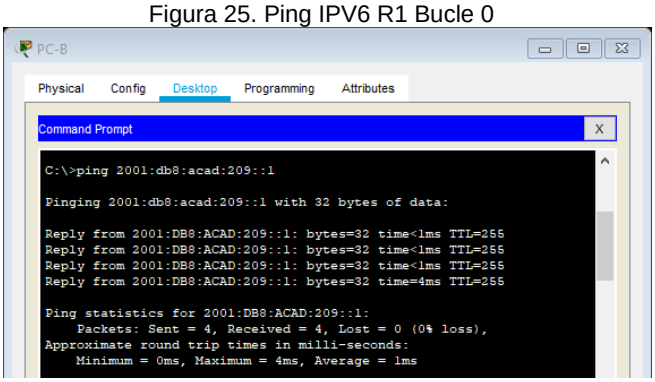
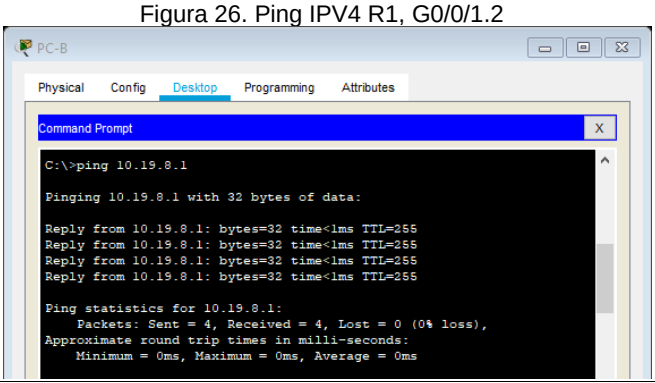
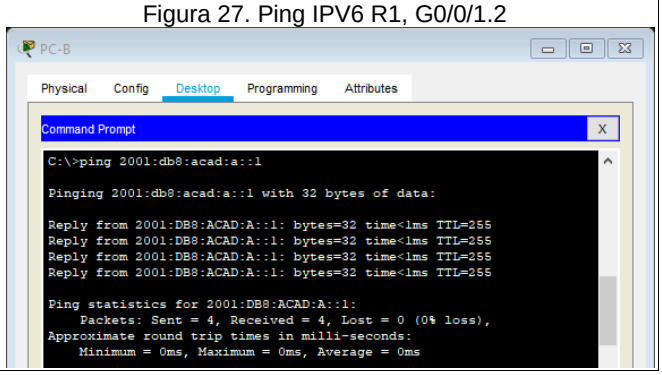
Tabla 7 – Pruebas de Conectividad

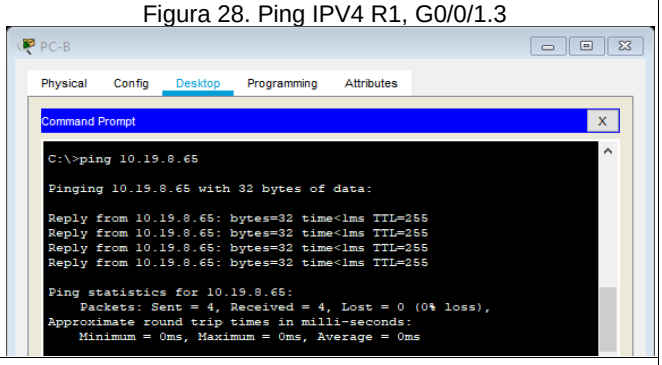
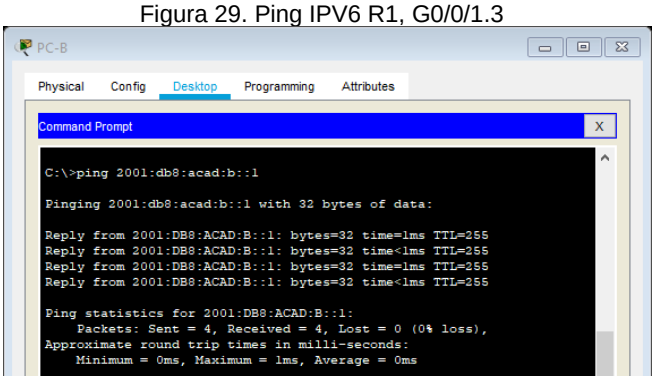
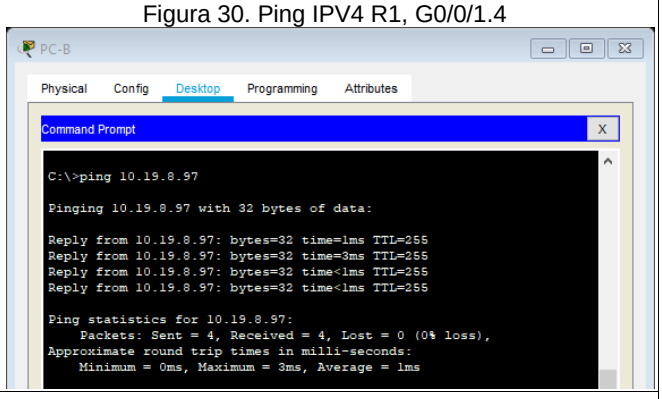
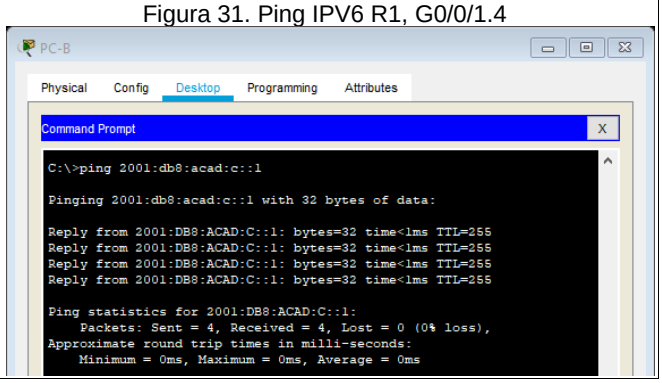
de Internet	Dirección IP	Resultados de ping
DESDE: PC-A → A: R1, G0/0/1.2		
Dirección	10.19.8.1	Figura 10. Ping IPV4 R1, G00/1.2 
IPv6	2001:db8:acad:a::1	Figura 11. Ping IPV6 R1, G0/0/1.2 
DESDE: PC-A → A: R1, G0/0/1.3		
Dirección	10.19.8.65	Figura 12. Ping IPV4 R1, G0/0/1.3 

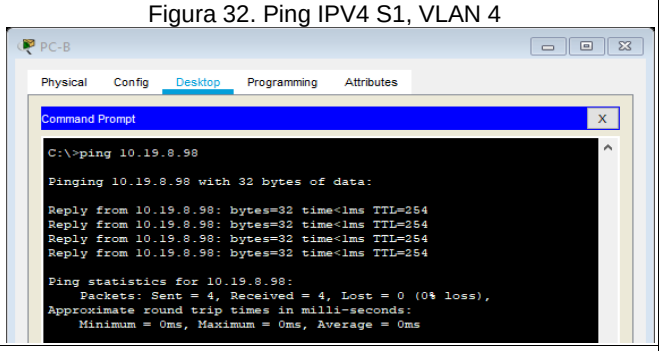
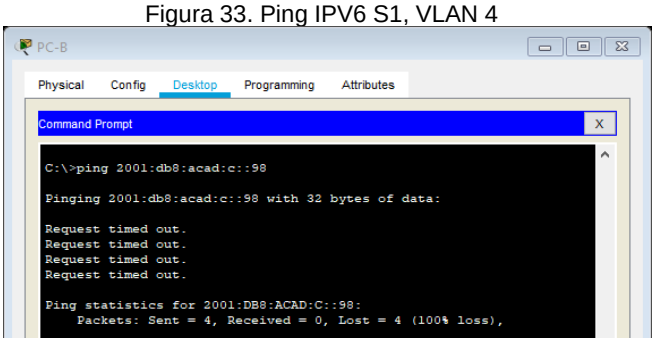
IPv6	2001:db8:acad:b::1	Figura 13. Ping IPV6 R1, G0/0/1.3 
DESDE: PC-A → A: R1, G0/0/1.4		
Dirección	10.19.8.97	Figura 14. Ping IPV4 R1, G00/1.4 
IPv6	2001:db8:acad:c::1	Figura 15. Ping IPV6 R1, G0/0/1.4 
DESDE: PC-A → A: S1, VLAN 4		
Dirección	10.19.8.98	Figura 16. Ping IPV4 S1, VLAN 4 

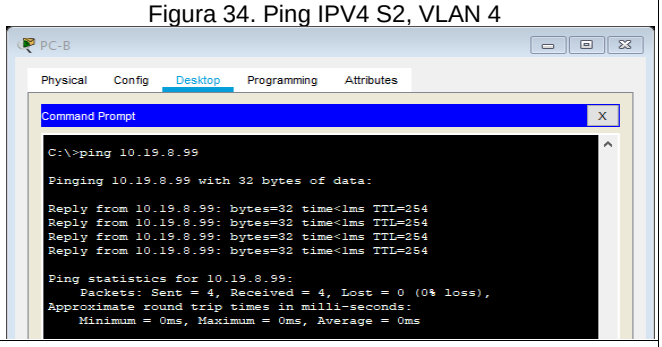
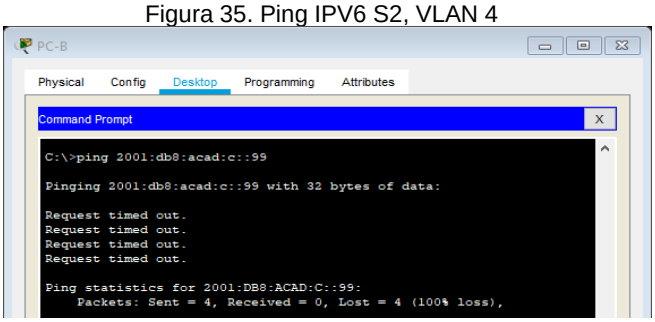
IPv6	2001:db8:acad:c: :98	Figura 17. Ping IPV6 S1, VLAN 4  Al realizar la prueba de Ping IPV6 a la SVI del S1 no es exitosa la tarea, se realizan validaciones, pero todo está OK, posible problema del Packet Tracer.
DESDE: PC-A → A: S2, VLAN 4		
Dirección	10.19.8.99	Figura 18. Ping IPV4 S2, VLAN 4 
IPv6	2001:db8:acad:c: :99	Figura 19. Ping IPV6 S2, VLAN 4  Al realizar la prueba de Ping IPV6 a la SVI del S2 no es exitosa la tarea, se realizan validaciones, pero todo está OK, posible problema del Packet Tracer.

<table>
<tr><th colspan="3">DESDE: PC-A → A: PC-B</th></tr>
<tr><td>Dirección</td><td>IP address will vary.</td><td>Figura 20. Ping IPV4 PC-B
 
</td></tr>
<tr><td>IPv6</td><td>2001:db8:acad:b: :50</td><td>Figura 21. Ping IPV6 PC-B
 
</td></tr>
<tr><th colspan="3">DESDE: PC-A → A: R1 Bucle 0</th></tr>
<tr><td>Dirección</td><td>209.165.201.1</td><td>Figura 22. Ping IPV4 R1 Bucle 0
 
</td></tr>
<tr><td>IPv6</td><td>2001:db8:acad:209: :1</td><td>Figura 23. Ping IPV6 R1 Bucle 0
 
</td></tr>
</table>

<table>
<tr><th colspan="3">DESDE: PC-B → A: R1 Bucle 0</th></tr>
<tr><td>Dirección</td><td>209.165.201.1</td><td>Figura 24. Ping IPV4 R1 Bucle 0
 
</td></tr>
<tr><td>IPv6</td><td>2001:db8:acad:209: :1</td><td>Figura 25. Ping IPV6 R1 Bucle 0
 
</td></tr>
<tr><th colspan="3">DESDE: PC-B → A: R1, G0/0/1.2</th></tr>
<tr><td>Dirección</td><td>10.19.8.1</td><td>Figura 26. Ping IPV4 R1, G0/0/1.2
 
</td></tr>
<tr><td>IPv6</td><td>2001:db8:acad:a: :1</td><td>Figura 27. Ping IPV6 R1, G0/0/1.2
 
</td></tr>
</table>

<table>
<tr><th colspan="3">DESDE: PC-B → A: R1, G0/0/1.3</th></tr>
<tr><td>Dirección</td><td>10.19.8.65</td><td>Figura 28. Ping IPV4 R1, G0/0/1.3
 
</td></tr>
<tr><td>IPv6</td><td>2001:db8:acad:b: :1</td><td>Figura 29. Ping IPV6 R1, G0/0/1.3
 
</td></tr>
<tr><th colspan="3">DESDE: PC-B → A: R1, G0/0/1.4</th></tr>
<tr><td>Dirección</td><td>10.19.8.97</td><td>Figura 30. Ping IPV4 R1, G0/0/1.4
 
</td></tr>
<tr><td>IPv6</td><td>2001:db8:acad:c: :1</td><td>Figura 31. Ping IPV6 R1, G0/0/1.4
 
</td></tr>
</table>

<table>
<tr><th colspan="3">DESDE: PC-B → A: S1, VLAN 4</th></tr>
<tr><td>Dirección</td><td>10.19.8.98</td><td>Figura 32. Ping IPV4 S1, VLAN 4
 
</td></tr>
<tr><td>IPv6</td><td>2001:db8:acad:c: :98</td><td>Figura 33. Ping IPV6 S1, VLAN 4
 

Al realizar la prueba de Ping IPV6 a la SVI del S1 no es exitosa la tarea, se realizan validaciones, pero todo está OK, posible problema del Packet Tracer.</td></tr>
<tr><th colspan="3">DESDE: PC-B → A: S2, VLAN 4</th></tr>
<tr><td>Dirección</td><td>10.19.8.99</td><td>Figura 34. Ping IPV4 S2, VLAN 4
 
</td></tr>
<tr><td>IPv6</td><td>2001:db8:acad:c: :99</td><td>Figura 35. Ping IPV6 S2, VLAN 4
 

Al realizar la prueba de Ping IPV6 a la SVI del S2 no es exitosa la tarea, se realizan validaciones, pero todo está OK, posible problema del Packet Tracer.</td></tr>
</table>

ESCENARIO 2

Figura 36. Escenario 2

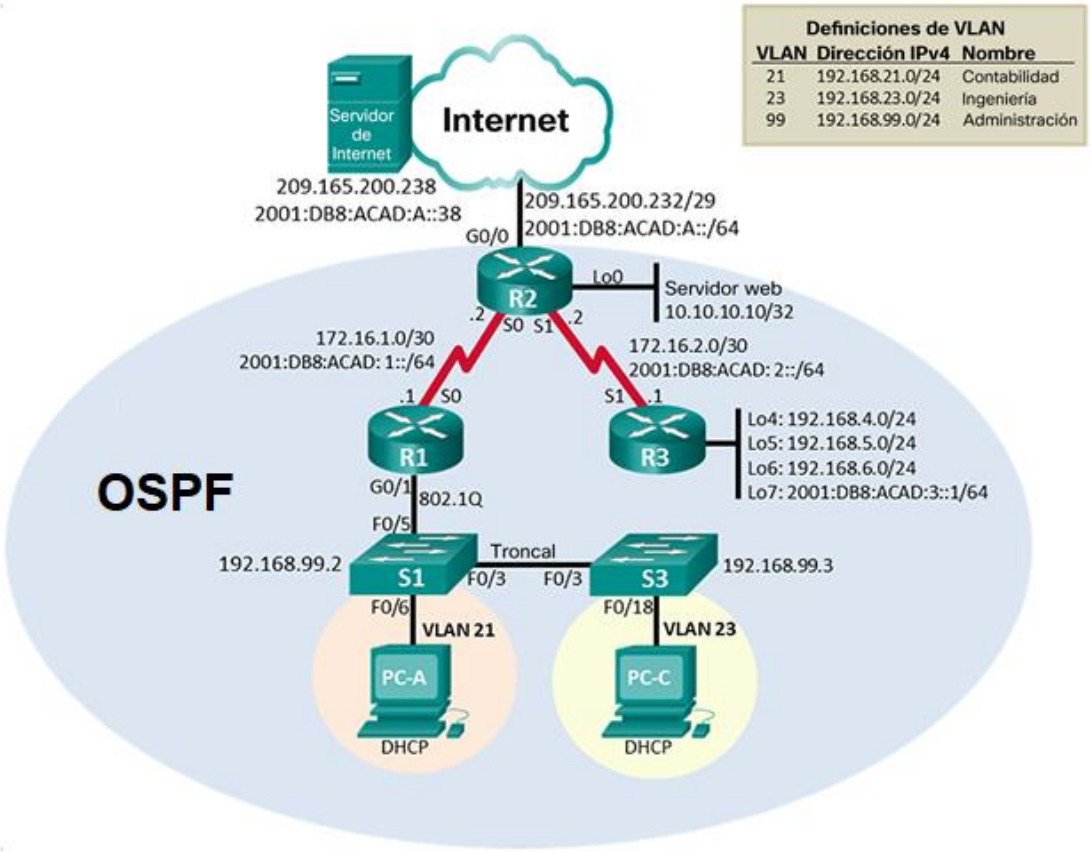
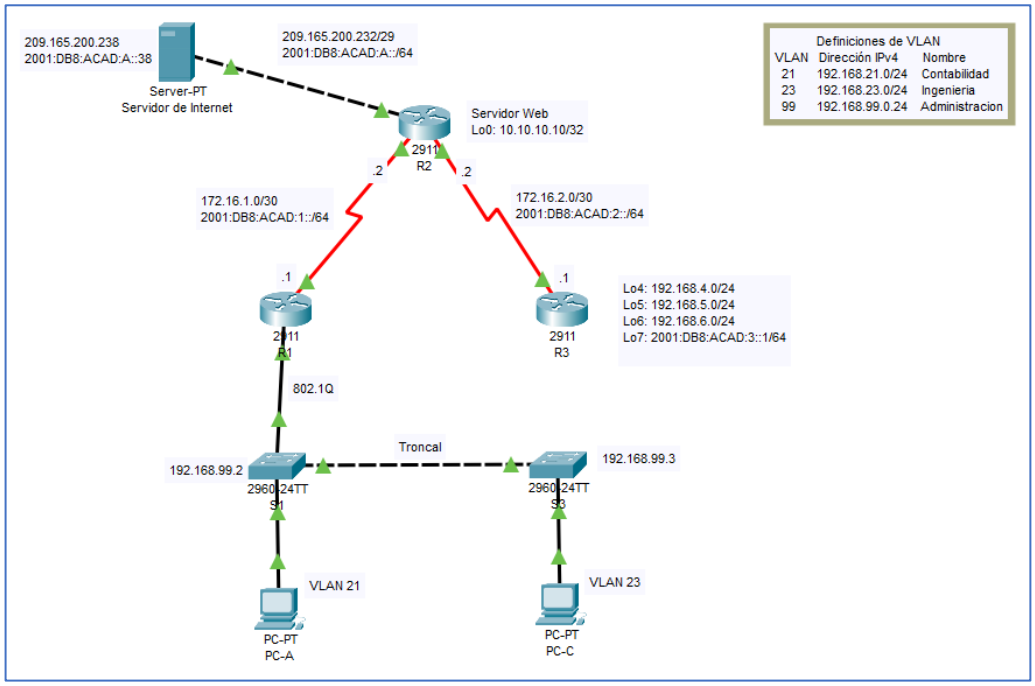


Figura 37. Simulación de escenario 2



1.1 Inicializar y volver a cargar los routers y los switches, Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.

En este primer paso en el desarrollo del segundo escenario, accedemos al router y a cada uno de los Switch para borrar las configuraciones que puedan haberse realizado, a continuación, anexo código.

Tabla 8 – Inicialización dispositivos

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router> Router>en Router#erase startup-config Continue? [confirm]y[OK]
Volver a cargar todos los routers	Router> Router>en Router#reload Proceed with reload? [confirm]y
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch> Switch>en Switch#erase startup-config Continue? [confirm]y[OK] Switch> Switch>en Switch#delete vlan.dat Switch#

Volver a cargar ambos switches	Switch> Switch>en Switch#reload Proceed with reload? [confirm]y
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch> Switch>en Switch#show flash: Switch#exit

2.1 Configurar la computadora de Internet, Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología).

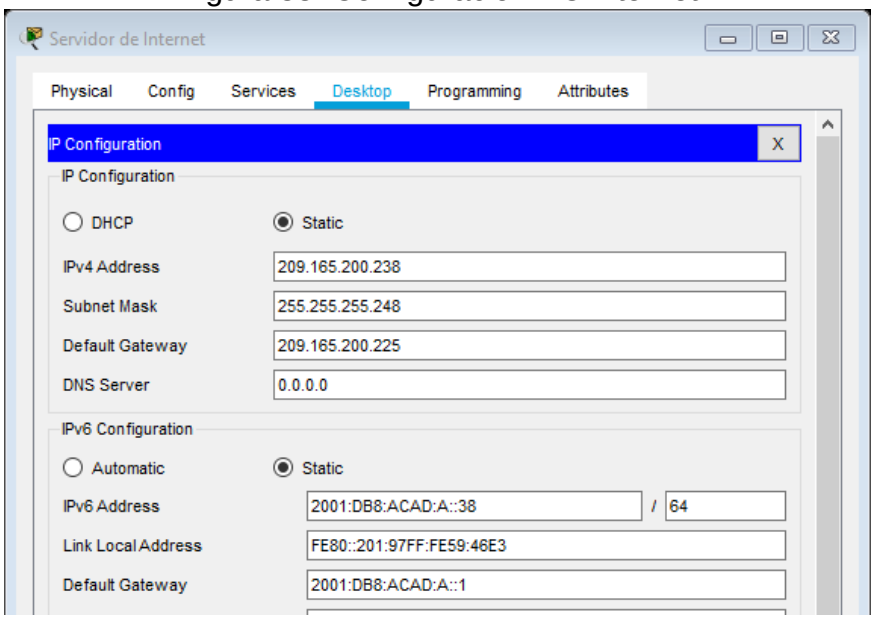
A continuación, se realiza la configuración IPv4 e IPv6 del servidor de internet de acuerdo con la siguiente tabla:

Tabla 9 – Configuración PC internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:A::1

Nota: se ajustan las especificaciones de acuerdo con la información encontrada en la topología ya que se presentaban diferencias en la tabla

Figura 38. Configuración PC internet



2.2 Configurar R1

En este paso aplicamos las primeras configuraciones al Router 1, entre las cuales encontramos el cambio de nombre, desactivación de la búsqueda por DNS, configuración de las contraseñas para EXEC, consola y telnet, además del cifrado de password, mensaje MOTD y configuración de Interfaz serial estableciendo direccionamiento IPv4 e IPv6, al igual que configurar las rutas predeterminadas.

A continuación, se presentan en la siguiente tabla las configuraciones realizadas al R1:

Tabla 10 – Configuración inicial R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>en Router #config t Router(config)# no ip domain-lookup Router(config)#end
Nombre del router	Router>en Router #config t Router(config)#hostname R1 R1(config)#end
Contraseña de exec privilegiado cifrada	R1>en R1#config t R1(config)#enable secret class R1(config)#end
Contraseña de acceso a la consola	R1>en R1#config t R1(config)#line con 0 R1(config-line)#password cisco R1(config-line)#login R1(config)#end
Contraseña de acceso Telnet	R1>en R1#config t R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#login R1(config)#end
Cifrar las contraseñas de texto no cifrado	R1>en R1#config t R1(config)#service password-encryption R1(config)#end

Mensaje MOTD	R1>en R1#config t R1(config)#banner motd # Se prohíbe el acceso no autorizado # R1(config)#end
Interfaz S0/0/0	R1>en R1#config t R1(config)#inter serial 0/0/0 R1(config-if)#ip add 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 add 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#description R2-Link R1(config-if)#no shut R1(config)#end
Rutas predeterminadas	R1>en R1#config t R1(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0 R1(config)#ipv6 route ::/0 serial 0/0/0 R1(config)#end

2.3 Configurar R2

En este paso aplicamos las primeras configuraciones al Router 2, entre las cuales encontramos el cambio de nombre, desactivación de la búsqueda por DNS, configuración de las contraseñas para EXEC, consola y telnet, habilitar el servicio HTTP, además del cifrado de password, mensaje MOTD y configuración de las Interfaz seriales, Simulación de internet y loopback estableciendo direccionamiento IPv4 e IPv6, al igual que configurar las rutas predeterminadas.

A continuación, se presentan en la siguiente tabla las configuraciones realizadas al R2:

Tabla 11 – Configuración inicial R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>en Router #config t Router(config)# no ip domain-lookup Router(config)#end

Nombre del router	Router>en Router #config t Router(config)#hostname R2 R2(config)#end
Contraseña de exec privilegiado cifrada	R2>en R2#config t R2(config)#enable secret class R2(config)#end
Contraseña de acceso a la consola	R2>en R2#config t R2(config)#line con 0 R2(config-line)#password cisco R2(config-line)#login R2(config)#end
Contraseña de acceso Telnet	R2>en R2#config t R2(config)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#login R2(config)#end
Cifrar las contraseñas de texto no cifrado	R2>en R2#config t R2(config)#service password-encryption R2(config)#end
Habilitar el servidor HTTP	R2>en R2#config t R2(config)#ip http-server R2(config)#end
Mensaje MOTD	R2>en R2#config t R2(config)#banner motd # Se prohíbe el acceso no autorizado# R2(config)#end
Interfaz S0/0/0	R2>en R2#config t R2(config)#inter s0/0/0 R2(config-if)#description R1-Link R2(config-if)#ip add 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 add 2001:db8:acad:1::2/64 R2(config-if)#no shut R2(config-if)#end

Interfaz S0/0/1	R2>en R2#config t R2(config)#inter s0/0/1 R2(config-if)#description R3-Link R2(config-if)#ip add 172.16.2.2 255.255.255.252 R2(config-if)#ipv6 add 2001:db8:acad:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no shut R2(config-if)#end
Interfaz G0/0 (simulación de Internet)	R2>en R2#config t R2(config)#inter gi0/0 R2(config-if)#description Internet R2(config-if)#ip add 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 add 2001:db8:acad:A::1/64 R2(config-if)#no shut R2(config-if)#end
Interfaz loopback 0 (servidor web simulado)	R2>en R2#config t R2(config-f)#interface loopback 0 R2(config-if)#description Servidor-Web R2(config-if)#ip add 10.10.10.10 255.255.255.255 R2(config-if)#end
Ruta predeterminada	R2>en R2#config t R2(config)#ip route 0.0.0.0 0.0.0.0 gi0/0 R2(config)#ipv6 route ::/0 gi0/0 R2(config)#end

2.4 Configurar R3

En este paso aplicamos las primeras configuraciones al Router 3, entre las cuales encontramos el cambio de nombre, desactivación de la búsqueda por DNS, configuración de las contraseñas para EXEC, consola y telnet, además del cifrado de password, mensaje MOTD y configuración de la Interfaz serial y loopback

estableciendo direccionamiento IPv4 e IPv6, al igual que configurar las rutas predeterminadas.

A continuación, se presentan en la siguiente tabla las configuraciones realizadas al R3:

Tabla 12 – Configuración inicial R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router>en Router #config t Router(config)# no ip domain-lookup Router(config)#end
Nombre del router	Router>en Router #config t Router(config)#hostname R3 R3(config)#end
Contraseña de exec privilegiado cifrada	R3>en R3#config t R3(config)#enable secret class R3(config)#end
Contraseña de acceso a la consola	R3>en R3#config t R3(config)#line con 0 R3(config-line)#password cisco R3(config-line)#login R3(config)#end
Contraseña de acceso Telnet	R3>en R3#config t R3(config)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login R3(config)#end
Cifrar las contraseñas de texto no cifrado	R3>en R3#config t R3(config)#service password-encryption R3(config)#end
Mensaje MOTD	R3>en R3#config t R3(config)#banner motd # Se prohibe el acceso no autorizado# R3(config)#end

Interfaz S0/0/1	R3>en R3#config t R3config)#inter s0/0/1 R3(config-if)#description R2-Link R3(config-if)#ip add 172.16.2.1 255.255.255.252 R3(config-if)#ipv6 add 2001:db8:acad:2::1/64 R2(config-if)#no shut R2(config-if)#end
Interfaz loopback 4	R3>en R3#config t R3(config)#interface loopback 4 R3(config-if)#ip add 192.168.4.1 255.255.255.0 R3(config-if)#end
Interfaz loopback 5	R3>en R3#config t R3(config)#interface loopback 5 R3(config-if)#ip add 192.168.5.1 255.255.255.0 R3(config-if)#end
Interfaz loopback 6	R3>en R3#config t R3(config)#interface loopback 6 R3(config-if)#ip add 192.168.6.1 255.255.255.0 R3(config-if)#end
Interfaz loopback 7	R3>en R3#config t R3(config)#interface loopback 7 R3(config-if)#ipv6 add 2001:db8:acad:3::1/64 R3(config-if)#end
Rutas predeterminadas	R3>en R3#config t R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1 R3(config-if)#end

2.5 Configurar S1

En este paso aplicamos las primeras configuraciones al Switch 1, entre las cuales encontramos el cambio de nombre, desactivación de la búsqueda por DNS, configuración de las contraseñas para EXEC, consola y telnet, además del cifrado de password y mensaje MOTD

A continuación, se presentan en la siguiente tabla las configuraciones realizadas al S1:

Tabla 13 – Configuración inicial S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch>en Switch#config t Switch(config)# no ip domain-lookup Switch(config)#end
Nombre del switch	Switch>en Switch#config t Switch(config)#hostname S1 S1(config)#end
Contraseña de exec privilegiado cifrada	S1>en S1#config t S1(config)#enable secret class S1(config)#end
Contraseña de acceso a la consola	S1>en S1#config t S1(config)#line con 0 S1(config-line)#password cisco S1(config-line)#login S1(config)#end
Contraseña de acceso Telnet	S1>en S1#config t S1(config)#line vty 0 4 S1(config-line)#password cisco S1(config-line)#login S1(config)#end
Cifrar las contraseñas de texto no cifrado	S1>en S1#config t S1(config)#service password-encryption S1(config)#end

Mensaje MOTD	S1>en S1#config ter S1(config)#banner motd # Se prohíbe el acceso no autorizado# S1(config)#end

2.6 Configurar S3

En este paso aplicamos las primeras configuraciones al Switch 3, entre las cuales encontramos el cambio de nombre, desactivación de la búsqueda por DNS, configuración de las contraseñas para EXEC, consola y telnet, además del cifrado de password y mensaje MOTD

A continuación, se presentan en la siguiente tabla las configuraciones realizadas al S3:

Tabla 14 – Configuración inicial S3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Switch>en Switch#config t Switch(config)# no ip domain-lookup Switch(config)#end
Nombre del switch	Switch>en Switch#config t Switch(config)#hostname S3 S3(config)#end
Contraseña de exec privilegiado cifrada	S3>en S3#config t S3(config)#enable secret class S3(config)#end
Contraseña de acceso a la consola	S3>en S3#config t S3(config)#line con 0 S3(config-line)#password cisco S3(config-line)#login S3(config)#end
Contraseña de acceso Telnet	S3>en S3#config t S3(config)#line vty 0 4 S3(config-line)#password cisco S3(config-line)#login S3(config)#end

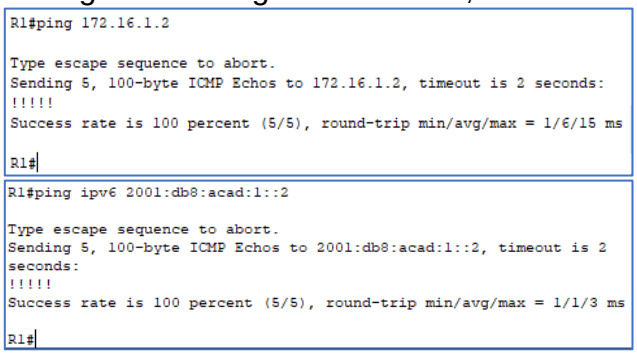
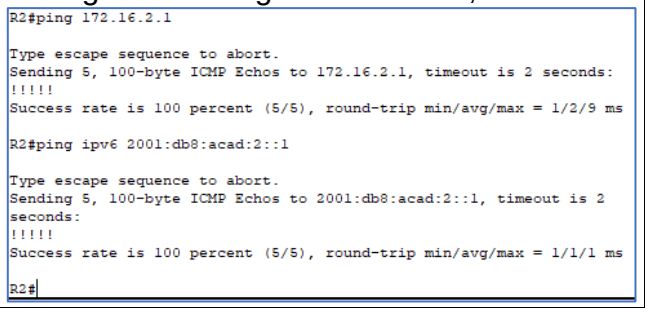
Cifrar las contraseñas de texto no cifrado	S3>en S3#config t S3(config)#service password-encryption S3(config)#end
Mensaje MOTD	S3>en S3#config t S3(config)#banner motd # Se prohíbe el acceso no autorizado# S3(config)#end

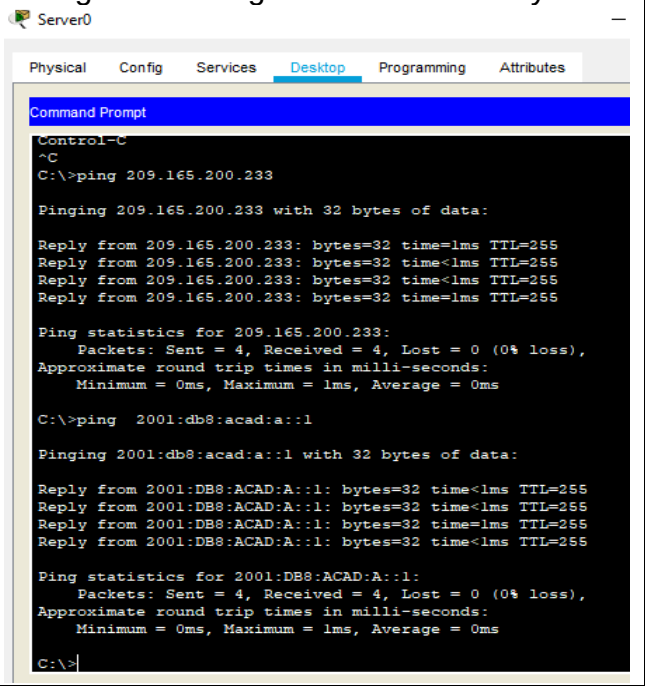
2.7 Verificar la conectividad de la red, Utilice el comando ping para probar la conectividad entre los dispositivos de red.

En este paso realizamos pruebas de conectividad con cada uno de los dispositivos de la red, a través del comando Ping validamos la conectividad.

A continuación, se presentan en la siguiente tabla las pruebas realizadas:

Tabla 15 – Pruebas de conectividad

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2 2001:db8:acad:1::2	Figura 39. Ping IPv4/IPv6 R2, S0/0/0 
R2	R3, S0/0/1	172.16.2.1 2001:db8:acad:2::1	Figura 40. Ping IPv4/IPv6 R3, S0/0/1 

PC de Internet	Gateway predeterminado	209.165.200.233 2001:db8:acad:a::1	Figura 41. Ping IPv4/IPv6 Gateway P. 

3.1 Configurar S1. Configurar la seguridad del switch, las VLAN y el Routing entre VLAN

En este paso realizamos la creación de las VLAN al tiempo que asignamos el direccionamiento IP y Gateway predeterminado, además, configuramos las troncales asignando la VLAN nativa, finalmente se configuran los puertos en modo de acceso y se apagan los puertos sin usar.

A continuación, se presentan en la siguiente tabla las configuraciones realizadas al S1

Tabla 16 – Configuraciones de seguridad S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1>en S1#config t S1(config)#vlan 21 S1(config)#name Contabilidad S1(config)#vlan 23 S1(config)#name Ingenieria S1(config)#vlan 99 S1(config)#name Administracion S1(config)#end

Asignar la dirección IP de administración.	S1>en S1#config t S1(config)#inter vlan 99 S1(config-if)#ip add 192.168.99.2 255.255.255.0 S1(config)#end
Asignar el Gateway predeterminado	S1>en S1#config t S1(config)#ip default-gateway 192.168.99.1 S1(config)#end
Forzar el enlace troncal en la interfaz F0/3	S1>en S1#config t S1(config)#inter fa0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#end
Forzar el enlace troncal en la interfaz F0/5	S1>en S1#config t S1(config)#inter fa0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#end
Configurar el resto de los puertos como puertos de acceso	S1>en S1#config t S1(config)#inter range fa0/1 - fa0/2 S1(config-if-range)#switchport mode access S1(config-if-range)#inter range fa0/7 - fa0/24 S1(config-if-range)#switchport mode access S1(config-if-range)#exit S1(config)#inter fa0/4 S1(config-if)#switchport mode access S1(config-if)#end
Asignar F0/6 a la VLAN 21	S1>en S1#config t S1(config)#inter fa0/6 S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 21 S1(config-if)#end

Apagar todos los puertos sin usar	S1>en S1#config t S1(config)#inter range fa0/1 - fa0/2 S1(config-if-range)#shut S1(config-if-range)#inter range fa0/7 - fa0/24 S1(config-if-range)#shut S1(config-if-range)#exit S1(config)#inter fa0/4 S1(config-if)#shut S1(config-if)#end

3.2 Configurar S3. Configurar la seguridad del switch, las VLAN y el Routing entre VLAN

En este paso realizamos la creación de las VLAN al tiempo que asignamos el direccionamiento IP y Gateway predeterminado, además, configuramos las troncales asignando la VLAN nativa, finalmente se configuran los puertos en modo de acceso, se asigna el Puerto Asignar F0/18 a la VLAN 23 y se apagan los puertos sin usar.

A continuación, se presentan en la siguiente tabla las configuraciones realizadas al S3

Tabla 17 – Configuraciones de seguridad S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3>en S3#config t S3(config)#vlan 21 S3(config)#name Contabilidad S3(config)#vlan 23 S3(config)#name Ingenieria S3(config)#vlan 99 S3(config)#name Administracion S3(config)#end
Asignar la dirección IP de administración	S3>en S3#config t S3(config)#inter vlan 99 S3(config-if)#ip add 192.168.99.3 255.255.255.0 S3(config)#end

Asignar el Gateway predeterminado.	S3>en S3#config t S3(config)#ip default-gateway 192.168.99.1 S3(config)#end
Forzar el enlace troncal en la interfaz F0/3	S3>en S3#config t S3(config)#inter fa0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1 S3(config-if)#end
Configurar el resto de los puertos como puertos de acceso	S3>en S3#config t S3(config)#inter range fa0/1 - fa0/2 S3(config-if-range)#switchport mode access S3(config-if-range)#inter range fa0/4 - fa0/17 S3(config-if-range)#switchport mode access S3(config-if-range)#inter range fa0/19 - fa0/24 S3(config-if-range)#switchport mode access S3(config-if)#end
Asignar F0/18 a la VLAN 23	S3>en S3#config t S3(config)#inter fa0/18 S3(config-if)#switchport mode access S3(config-if)#switchport access vlan 23 S3(config-if)#end
Apagar todos los puertos sin usar	S3>en S3#config t S3(config)#inter range fa0/1 - fa0/2 S3(config-if-range)#shut S3(config-if-range)#inter range fa0/4 - fa0/17 S3(config-if-range)#shut S3(config-if-range)#inter range fa0/19 - fa0/24 S3(config-if-range)#shut S3(config-if)#end

3.3 Configurar R1. Configurar la seguridad del switch, las VLAN y el Routing entre VLAN

En este paso realizamos la configuración de las subinterfaces 802.1Q en G0/1 y activación de la interfaz

A continuación, se presentan en la siguiente tabla las configuraciones realizadas al R1

Tabla 18 – Configuraciones de subinterfaces R1

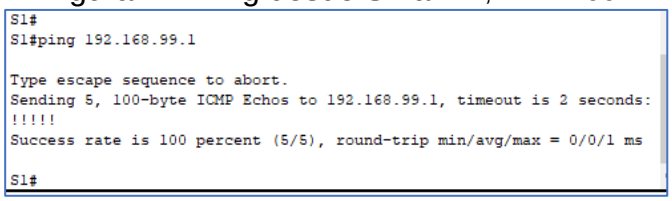
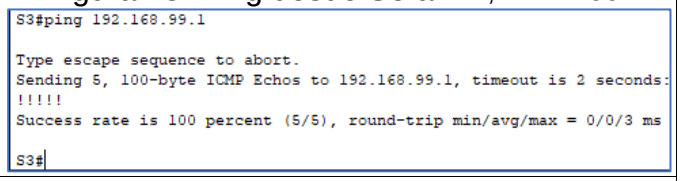
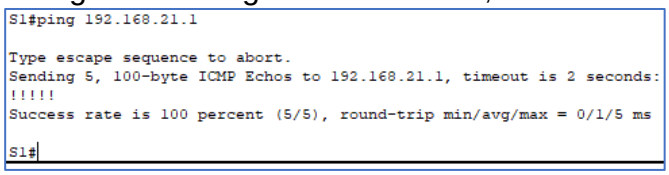
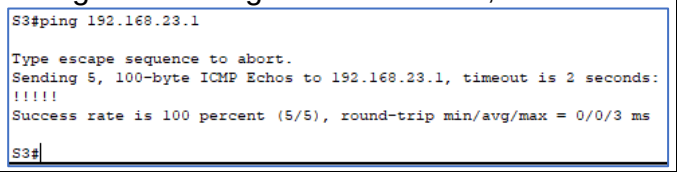
Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1>en R1#config t R1(config)#inter gi0/1.21 R1(config-if)#des LAN de Contabilidad R1(config-if)#encap dot1q 21 R1(config-subif)#ip add 192.168.21.1 255.255.255.0 R1(config-subif)#end
Configurar la subinterfaz 802.1Q .23 en G0/1	R1>en R1#config t R1(config)#inter gi0/1.23 R1(config-if)#des LAN de Ingenieria R1(config-if)#encap dot1q 23 R1(config-subif)#ip add 192.168.23.1 255.255.255.0 R1(config-subif)#end
Configurar la subinterfaz 802.1Q .99 en G0/1	R1>en R1#config t R1(config)#inter gi0/1.99 R1(config-if)#des LAN de Administracion R1(config-if)#encap dot1q 99 R1(config-subif)#ip add 192.168.99.1 255.255.255.0 R1(config-subif)#end
Activar la interfaz G0/1	R1>en R1#config t R1(config)#inter gi0/1 R1(config)#no shut R1(config)#end

3.4 Verificar la conectividad de la red, Utilice el comando ping para probar la conectividad entre los switches y el R1.

En este paso realizamos pruebas de conectividad entre los switches y el R1, a través del comando Ping validamos la conectividad.

A continuación, se presentan en la siguiente tabla las pruebas realizadas:

Tabla 19 – Pruebas de conectividad Switches y R1

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	Figura 42. Ping desde S1 al R1, VLAN 99 
S3	R1, dirección VLAN 99	192.168.99.1	Figura 43. Ping desde S3 al R1, VLAN 99 
S1	R1, dirección VLAN 21	192.168.21.1	Figura 44. Ping desde S1 al R1, VLAN 21 
S3	R1, dirección VLAN 23	192.168.23.1	Figura 45. Ping desde S3 al R1, VLAN 23 

4.1 Configurar OSPF en el R1. Configurar el protocolo de Routing dinámico OSPF

En este paso realizamos la configuración del protocolo OSPF en el R1, al tiempo que informamos las redes conectadas directamente, se establecen las interfaces LAN como pasivas y se Desactiva la sumarización automática

A continuación, se presentan en la siguiente tabla las configuraciones realizadas al R1

Tabla 20 – Configuración protocolo OSPF

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R1>en R1#config t R1(config)#router ospf 1 R1(config-router)#end
Anunciar las redes conectadas directamente	R1>en R1#config t R1(config)#router ospf 1 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0 R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#end
Establecer todas las interfaces LAN como pasivas	R1>en R1#config t R1(config)#router ospf 1 R1(config-router)#passive-interface gigabitEthernet 0/1 R1(config-router)#end
Desactive la sumarización automática	*En las siguientes configuraciones, la máscara deshabilita el resumen automático para el protocolo de enrutamiento OSPF. R1>en R1#config t R1(config)#router ospf 1 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0 R1(config-router)#network 172.16.1.0 0.0.0.3 area 0 R1(config-router)#end

4.2 Configurar OSPF en el R2. Configurar el protocolo de Routing dinámico OSPF

En este paso realizamos la configuración del protocolo OSPF en el R2, al tiempo que informamos las redes conectadas directamente, se establecen las interfaces LAN como pasivas y se Desactiva la sumarización automática

A continuación, se presentan en la siguiente tabla las configuraciones realizadas al R2

Tabla 21 – Configuración protocolo OSPF R2

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R2>en R2#config t R2(config)#router ospf 1 R2(config-router)#end
Anunciar las redes conectadas directamente	R2>en R2#config t R2(config)#router ospf 1 R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R2(config-router)#end
Establecer la interfaz LAN (loopback) como pasiva	R2>en R2#config t R2(config)#router ospf 1 R2(config-router)#passive-interface loopback 0 R2(config-router)#end
Desactive la sumarización automática.	*En las siguientes configuraciones, la máscara deshabilita el resumen automático para el protocolo de enrutamiento OSPF. R2>en R2#config t R2(config)#router ospf 1 R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R2(config-router)#end

4.3 Configurar OSPF en el R3. Configurar el protocolo de Routing dinámico OSPF

En este paso realizamos la configuración del protocolo OSPF en el R3, al tiempo que informamos las redes conectadas directamente, se establecen las interfaces LAN como pasivas y se Desactiva la sumarización automática

A continuación, se presentan en la siguiente tabla las configuraciones realizadas al R3

Tabla 22 – Configuración protocolo OSPF R3

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	R3>en R3#config t R3(config)#router ospf 1 R3(config-router)#end
Anunciar redes IPv4 conectadas directamente	R3>en R3#config t R3(config)#router ospf 1 R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#end
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3>en R3#config ter R3(config)#router ospf 1 R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6 R3(config-router)#passive-interface loopback 7 R3(config-router)#end
Desactive la sumarización automática.	R3>en R3#config ter R3(config)#router ospf 1 R3(config-router)#network 172.16.2.0 0.0.0.3 area 0 R3(config-router)#end

4.4 Verificar la información de OSPF.

En este paso realizamos la validación de la configuración realizada al protocolo OSPF

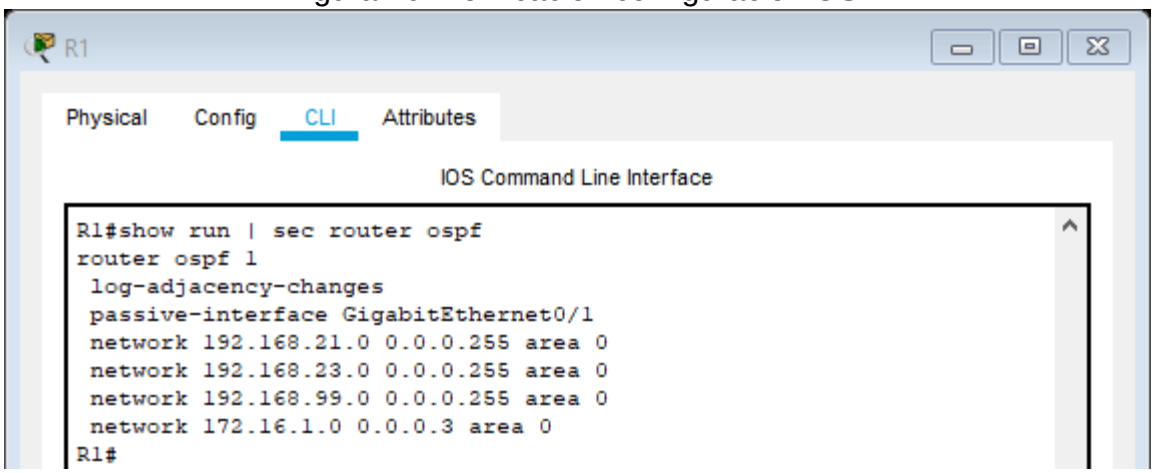
A continuación, se presentan en la siguiente tabla los comandos utilizados para validar las configuraciones al protocolo OSPF

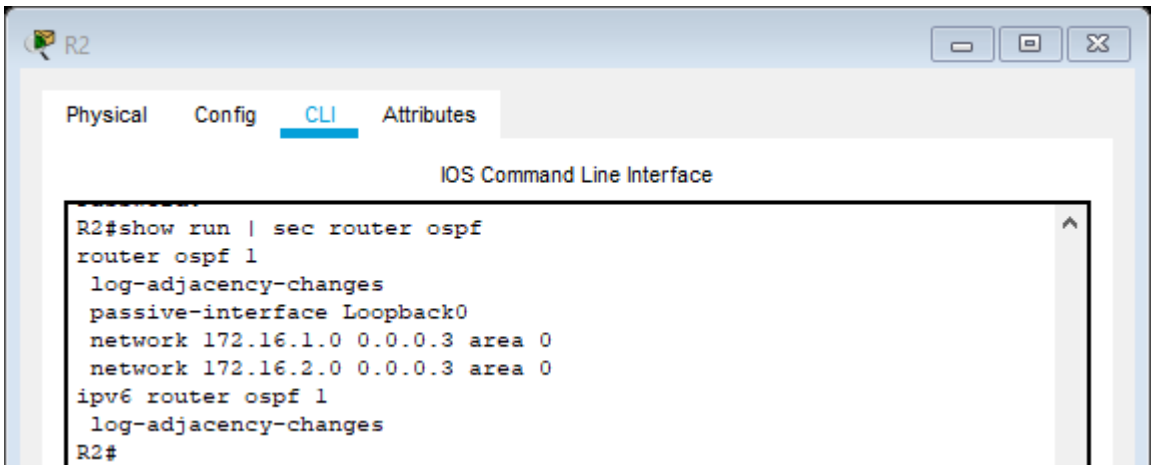
Tabla 23 – Comandos protocolo OSPF

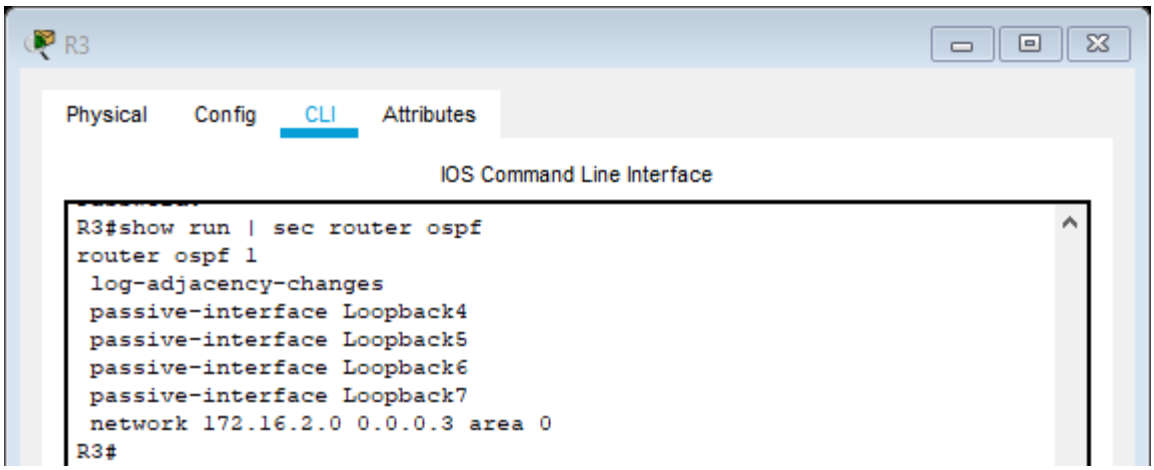
Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de Routing y las interfaces pasivas configuradas en un router?	show ip ospf interface
¿Qué comando muestra solo las rutas OSPF?	show ip route ospf

¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	show run | sec router ospf

Figura 46. Verificación configuración OSPF







5.1 Implementar DHCP y NAT para IPv4. Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

En este paso en el R1, realizamos la reserva de direcciones IP y creación del pool de DHCP en las VLAN solicitadas,

A continuación, se presentan en la siguiente tabla las configuraciones realizadas al R1

Tabla 24 – DHCP y NAT R1

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	R1>en R1#config t R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20 R1(config)#end
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	R1>en R1#config t R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20 R1(config)#end
Crear un pool de DHCP para la VLAN 21.	R1>en R1#config t R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#end
Crear un pool de DHCP para la VLAN 23	R1>en R1#config t R1(config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#end

5.2 Configurar la NAT estática y dinámica en el R2.

En este paso en el R2, realizamos la creación de un usuario local, habilitamos el servicio HTTP y se crea la NAT estática, asignando la interfaz interna y externa, al tiempo que la configuramos dentro de una ACL privada, además de definir el pool de direcciones IP públicas y la traducción de la NAT dinámica.

A continuación, se presentan en la siguiente tabla las configuraciones realizadas al R2

Tabla 25 – NAT estática y dinámica R2

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	R2>en R2#config t R2(config)#username webuser privilege 15 password cisco123 R2(config)#end
Habilitar el servicio del servidor HTTP	R2>en R2#config t R2(config)#ip http server R2(config)#end
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2>en R2#config t R2(config)#ip http authentication local R2(config)#end
Crear una NAT estática al servidor web.	R2>en R2#config t R2(config)#ip nat inside source static 209.165.200.233 209.165.200.229 R2(config)#end
Asignar la interfaz interna y externa para la NAT estática	R2>en R2#config t R2(config)#inter gi0/0 R2(config-if)#ip nat outside R2(config-if)exit R2(config)#inter s0/0/0 R2(config-if)#ip nat inside R2(config-if)#end

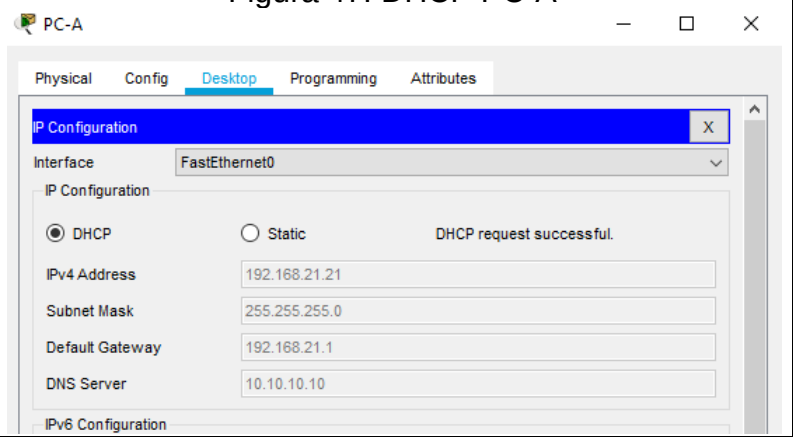
Configurar la NAT dinámica dentro de una ACL privada	R2>en R2#config t R2(config)#ip access-list standard 1 R2(config-std-nacl)#permit 192.168.21.0 0.0.0.255 R2(config-std-nacl)#permit 192.168.23.0 0.0.0.255 R2(config-std-nacl)#exit R2(config)#inter s0/0/1 R2(config-if)#outside R2(config-if)#end
Defina el pool de direcciones IP públicas utilizables.	R2>en R2#config t R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248 R2(config)#end
Definir la traducción de NAT dinámica	R2>en R2#config t R2(config)#ip nat inside source list 1 pool INTERNET R2(config)#end

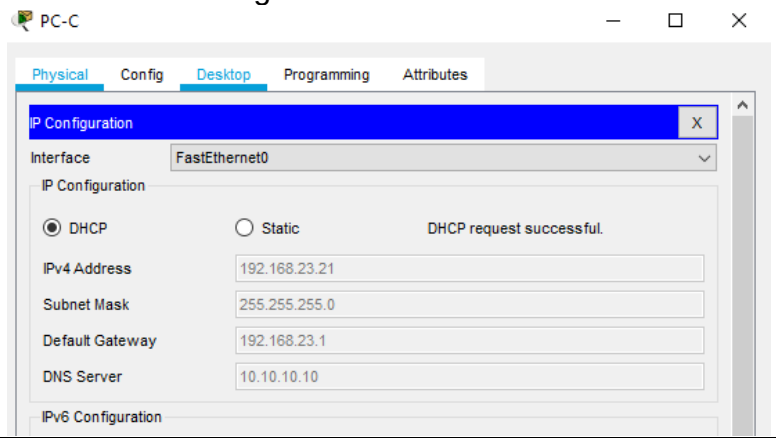
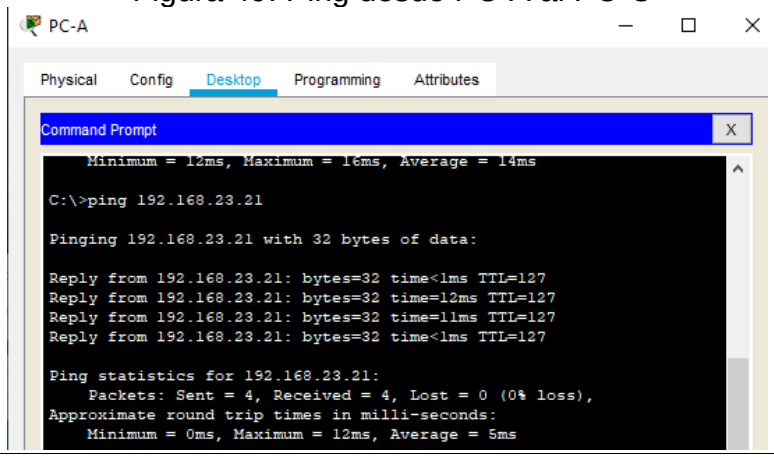
5.3 Verificar el protocolo DHCP y la NAT estática

En este paso realizamos una serie de verificaciones para validar las configuraciones de DHCP y NAT aplicadas.

A continuación, se presentan en la siguiente tabla las pruebas realizadas.

Tabla 26 – Verificación DHCP y la NAT

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Figura 47. DHCP PC-A 

Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Figura 48. DHCP PC-C 
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Figura 49. Ping desde PC-A al PC-C 
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	No es posible anexar Screnshot porque el Router aunque permite Setear las configuración para el servicio HTTP, no lo soporta.

6. Configurar NTP

En este paso realizamos la configuración NTP en el R1 y R2

A continuación, se presentan en la siguiente tabla las configuraciones realizadas.

Tabla 27 – configuración NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en	R2>en R2#clock set 09:00:00 March 5 2016 R2#exit
Configure R2 como un maestro NTP.	R2>en R2#config t R2(config)#ntp master 5 R2(config)end
Configurar R1 como un cliente NTP.	R1>en R1#config t R1(config)#ntp server 172.16.1.2 R2(config)end
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	R1>en R1#config t R1(config)#ntp update-calendar R2(config)end
Verifique la configuración de NTP en R1.	Figura 50. Validación configuración NTP R1

```
R1#show ntp associations

address         ref clock       st   when     poll    reach  delay
offset            disp
*~172.16.1.2    127.127.1.1     5    2        16      1      9.00
-3.00             0.00
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~
configured
R1#
```

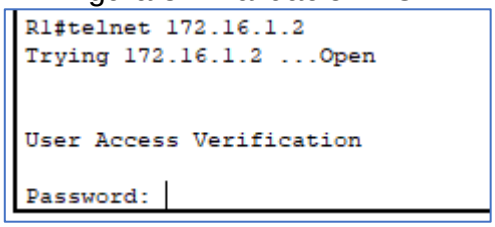
7 configurar y verificar las listas de control de acceso (ACL)

7.1 Restringir el acceso a las líneas VTY en el R2

En este paso realizamos la configuración de la lista de acceso donde permita que solo R1 pueda realizar conexión vía Telnet al R2, además se aplica la ACL a las VTY.

A continuación, se presentan en la siguiente tabla las configuraciones realizadas.

Tabla 28 – ACL R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	R2>en R2#config t R2(config)#ip access-list extended ADMIN-MGT R2(config-ext-nacl)#permit ip host 172.16.1.1 any R2(config-ext-nacl)end
Aplicar la ACL con nombre a las líneas VTY	R2>en R2#config t R2(config)#line vty 0 4 R2(config-line)#access-class ADMIN-MGT in R2(config-line)#end
Permitir acceso por Telnet a las líneas de VTY	R2>en R2#config t R2(config)#line vty 0 4 R2(config-line)#transport input telnet R2(config-line)#end
Verificar que la ACL funcione como se espera	Figura 51. Validación ACL 

7.2 Introducir el comando de CLI adecuado

En este paso se indica los comandos necesarios para consultas de ACL y NAT

A continuación, se presentan en la siguiente tabla los comandos solicitados.

Tabla 29 – Comandos ACL y NAT

Descripción del commando	(comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	show ip access-lists show ip access-lists <acl number> show ip access-lists <acl name>
Restablecer los contadores de una lista de acceso	clear access-list counters clear access-list counters <acl number> clear access-list counters <acl name>
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	show ip interface

¿Con qué comando se muestran las traducciones NAT?	show ip nat translations
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	clear ip nat translation *

CONCLUSIONES

En el primer escenario una de las tareas sencillas que se realizan al comienzo, pero que considero importante, consiste en asignar contraseñas al Router y Switch en su modo EXEC y acceso a la consola, acompañados por el cifrado de las contraseñas y estableciendo la longitud mínima a estas, de esta manera agregamos niveles de seguridad.

En el segundo escenario me pareció interesante saber que el protocolo de Routing dinámico OSPF nos ayuda a establecer la ruta idónea, al tiempo que utiliza IP Multicast para enviar actualizaciones de estado de link que ofrecen una descripción de esa interfaz y su relación con los routers vecinos, además no tiene limitación para el conteo de saltos y permite un mejor balanceo de carga.

Otra medida de control y seguridad interesante son las listas de acceso, al configurar la reglas nos permiten realizar una especie de filtro al trafico de la red, mejorando los niveles de seguridad al permitir o negar el acceso a recursos específicos.

Puedo concluir que el desarrollo de los escenarios es una práctica bastante exigente, debido que los conocimientos adquiridos deben ser sólidos y haber entendido muy bien todo el temario.

Durante el desarrollo del laboratorio tuve que apoyarme en las fuentes bibliográficas propuesta en el curso y en algunas externas validando que la información presentada sea de fuentes confiables.

El elaborar estas prácticas en Packet Tracer me permitió tener un acercamiento más profundo en lo relacionado a la configuración de dispositivos de comunicaciones, al igual que aclarar dudas sobre las diferentes pruebas a realizar para validar las configuraciones aplicadas.

A lo largo de la actividad tuve la oportunidad de aprender varios comandos muy utilices que me permitirán analizar, diagnosticar y corregir problemas a nivel de red y configuración de dispositivos.

A medida que avanzaba en el desarrollo de los escenarios tuve que ir reforzando temas como los fueron EtherChannel, port-security, OSPF, NAT y ACL.

BIBLIOGRAFIA

CISCO, Cisco (2018). Configuración de la dirección IPv4 de la interfaz VLAN en un switch Sx350 o SG350X a través de la CLI. https://www.cisco.com/c/es_mx/support/docs/smb/switches/cisco-350-series-managed-switches/smb5722-configure-vlan-interface-ipv4-address-on-an-sx350-or-sg350x.html

CISCO, Cisco (2020). Configure el puerto a las configuraciones del interfaz del VLAN en un conmutador con el CLI. https://www.cisco.com/c/es_mx/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb5653-configure-port-to-vlan-interface-settings-on-a-switch-throug.html

Cisco, Cisco. (2005). Recuperado en noviembre de 2020, Guía de diseño de OSPF. https://www.cisco.com/c/es_mx/support/docs/ip/open-shortest-path-first-ospf/7039-1.html

Ccnadesdecero, Alex W. (s.f.). Recuperado en noviembre de 2020, Configuración de Rutas Estáticas y Predeterminadas. https://ccnadesdecero.es/configuracion-rutas-estaticas-predeterminadas/#2_Configuracion_de_rutas_predeterminadas_IPv4

DelfiRosales, D.R. (s.f.). Recuperado en noviembre de 2020, Autenticación, utilizando la Base de Datos Local. https://delfirosales.blogspot.com/2014/04/autenticacion-utilizando-la-base-de.html

El Mundo en Bits, Javier (2013). CISCO, ESTABLECER LONGITUD DE UNA CONTRASEÑA. https://www.elmundoenbits.com/2013/03/cisco-passwd-length.html#.X4zCPdBKiUk

Interpolados, Admin (2017). CONFIGURACIÓN DE ENLACES TRONCALES IEEE 802.1Q. https://interpolados.wordpress.com/2017/05/01/configuracion-de-enlaces-troncales-ieee-802-1q/

Mikroways, Leandro D.T. (2009). SEGURIDAD DE PUERTO EN SWITCHES CISCO. https://www.mikroways.net/2009/11/26/seguridad-de-puerto-en-switches-cisco/

Página Web. (s.f.). En amazonaws. Recuperado en noviembre de 2020, Configuración inicial de un router, Configuración básica de un router. https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/4.1.3.4/4.1.3.4.html

Página Web. (s.f.). En netcloudengineering. Recuperado en noviembre de 2020. Configuración de una VLAN en Cisco Switch. https://netcloudengineering.com/configuracion-vlan-cisco-switch/

Página Web. (s.f.). En Sites Google. Recuperado en noviembre de 2020, Configuración del acceso mediante SSH. https://sites.google.com/site/redeslocalesyglobales/4-configuracion-de-red/2-configuracion-de-routers/3-configuracion-del-router/2-configuracion-de-los-accesos-al-router/ddddd

Página Web. (s.f.). En Sites Google. Recuperado en noviembre de 2020, Enlaces Troncales de las VLAN. https://sites.google.com/site/paginamodulo3vlan/3-2-enlaces-troncales

Página Web. (s.f.). En Wikipedia. Recuperado en noviembre de 2020, Lista de control de acceso, de https://es.wikipedia.org/wiki/Lista_de_control_de_acceso

Página Web. (s.f.). En Wikipedia. Recuperado en noviembre de 2020, Traducción de direcciones de red, de https://es.wikipedia.org/wiki/Traducci%C3%B3n_de_direcciones_de_red

Utez, (s.f.). Recuperado en noviembre de 2020, Configuración de contraseñas de router. http://www.utez.edu.mx/curriculas/ccna2_ES/CHAPID=knet-1076516759217/RLOID=knet1076516759778/RIOID=knet1076516760900/knet/1076516759217/ resourcecontent.html

Utez, (s.f.). Recuperado en noviembre de 2020, Práctica de laboratorio 3.1.3 Configuración de contraseñas del router. http://www.utez.edu.mx/curriculas/ccna2_ES/pdf/knet-1076521136351/CCNA2_lab_3_1_3_es.pdf